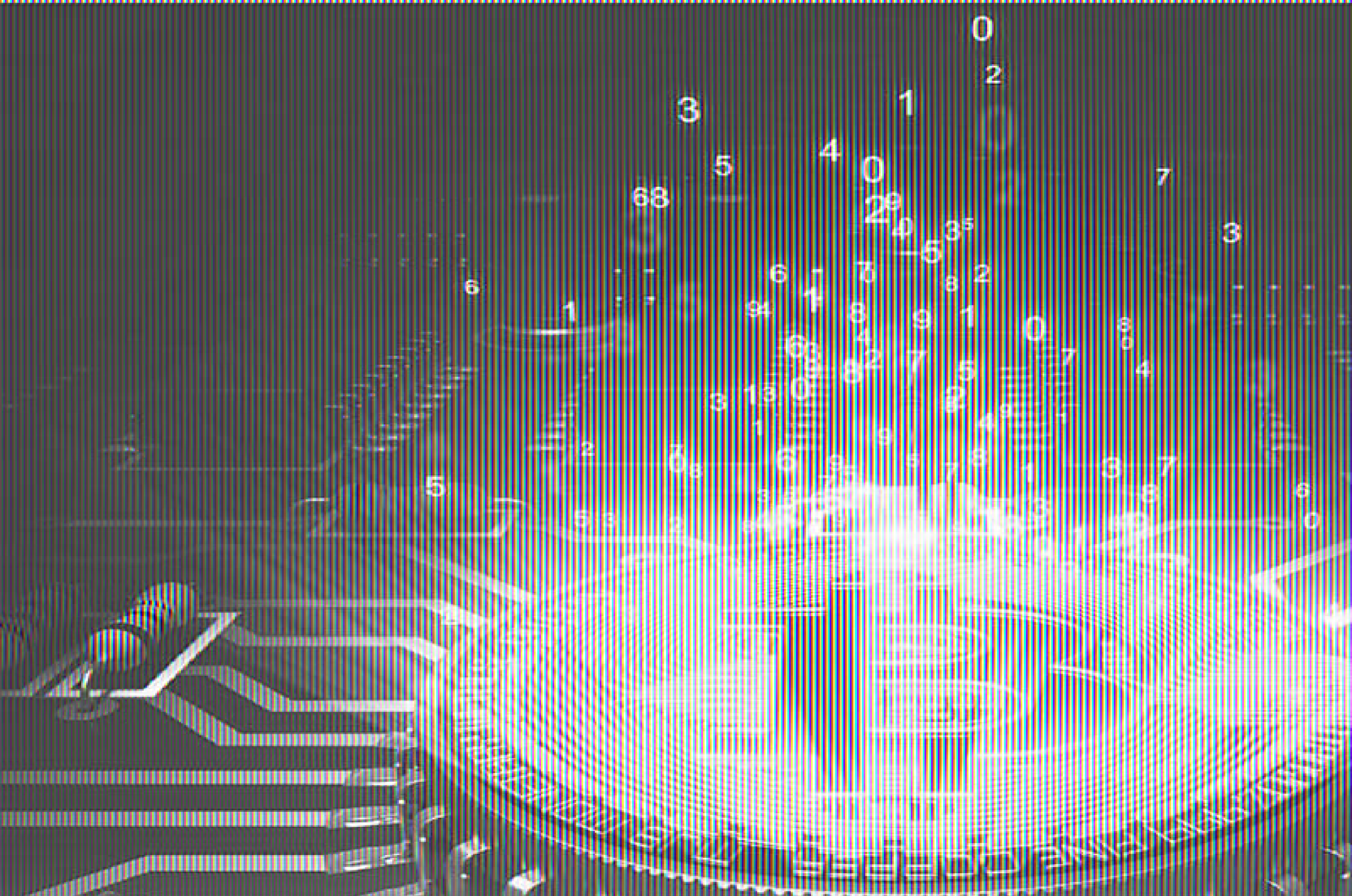
BITCOI

BONG BÓNG TÀI CHÍNH HAY TƯƠNG LAI



M A R K G A T E S

Bùi Đức Anh *dịch*

1980 BOOKS

NHÀ XUẤT BẢN
ĐẠI HỌC KINH TẾ QUỐC DÂN

Mục lục

Thông tin trong cuốn sách này chỉ phục vụ cho mục đích tham khảo chung. Mọi nội dung trình bày trong sách không nên coi là tư vấn và khuyến nghị.

Bạn nên cân nhắc các chỉ dẫn về luật pháp, tài chính và thuế vụ của mọi thông tin trong sách này dưới góc độ hoàn cảnh và tình huống riêng của bạn.

Mặc dù cuốn sách đã được chuẩn bị kỹ lưỡng và thận trọng, nhưng nhà xuất bản không chịu trách nhiệm với bất cứ lỗi sai, thiếu sót hoặc tổn thất phát sinh do áp dụng thông tin được cung cấp trong tài liệu này.

Tác giả và đơn vị xuất bản không chịu trách nhiệm với bất cứ thiệt hại nào, vì lý do sơ suất hay không, phát sinh từ việc sử dụng hoặc lạm dụng, trực tiếp hay gián tiếp, các thông tin trong sách.

Xin vui lòng liên hệ với tác giả nếu bạn phát hiện bất kỳ thiếu sót nào trong cuốn sách này

Tác giả, các cộng sự và đơn vị xuất bản đã rất nỗ lực để đảm bảo chất lượng và tính chính xác cho các nội dung của cuốn sách, nhưng có thể không tránh được một vài thiếu sót không đáng có.

Chúng tôi đánh giá rất cao việc bạn liên hệ và phản hồi khi phát hiện bất cứ thiếu sót nào trong nội dung sách trước khi thực hiện hành động nào khác. Vì thế, xin vui lòng liên hệ với chúng tôi theo địa chỉ sau để chúng tôi có thể chỉnh sửa càng sớm càng tốt: errors@wisefoxpub.com

Ghi chú về các đường dẫn trang web

Nhiều địa chỉ trang web được sử dụng trong cuốn sách này được rút gọn để giúp mọi người dễ dàng gõ trên máy tính và truy cập, đặc biệt khi cuốn sách được xuất bản dưới dạng bìa mềm.

Một ví dụ về cách đường dẫn được rút gọn trong cuốn sách này như sau:

Địa chỉ trang web gốc:

https://blockzzchain.info/block/000000000000000000e589576a954ac374d0a98478007a82f2a-57f76e243ece3

Địa chỉ trang web rút gọn: www.bitly.com/bitBlock1

Một số đường dẫn trang website chúng tôi cung cấp có thể chứa các liên kết khác phù hợp, nhưng sẽ không ảnh hưởng đến bất cứ nội dung nào được viết về các công ty này.

Các đường dẫn này cung cấp các tài liệu tham khảo thêm để bạn sử dụng và giúp ích cho bạn khi tương tác với trang web hay dịch vụ nào được đề cập trong cuốn sách.

Giới thiệu tác giả

Mark Gates lớn lên ở California và đóng vai trò quan trọng trong bức tranh công nghệ suốt hơn một thập kỷ.

Thời trung học, ông đã bắt đầu thiết kế web bằng cách sử dụng ngôn ngữ lập trình HTML và văn bản thuần túy trong Notepad trước khi xuất hiện các công cụ tiên tiến. Mark bắt đầu kinh doanh thiết kế web tại trường đại học vào thời gian bùng nổ Internet cách đây 15 năm.

Mark đã mở rộng kinh doanh thiết kế web thành hoạt động tiếp thị số, SEO và các phương tiện truyền thông xã hội. Sau khi sang nhượng doanh nghiệp này, ông dành thời gian để đi khắp nơi trên thế giới và kiếm tiền chỉ từ máy tính xách tay.

Mặc dù ban đầu rất hoài nghi về tiền mã hóa, nhưng Mark đã trở thành người ủng hộ mạnh mẽ các công nghệ dựa trên nền tảng Blockchain và tiền mã hóa.

Mark tin rằng cách học tốt nhất là trải nghiệm thực tế. Ông thích khám phá mọi thứ liên quan đến công nghệ, thu nhận kiến thức thực tiễn và truyền đạt cho mọi người để họ có thể làm được như vậy, cho dù người đó đang điều hành trang web, tiếp thị doanh nghiệp, kinh doanh tiền mã hóa, học lập trình hay tìm kiếm các kỹ năng thực tế để có được công việc mơ ước.

Mark luôn viết sách với bằng ngôn ngữ dễ hiểu kèm theo nhiều ví dụ hay hướng dẫn thực hành để giúp bạn đạt được mục tiêu của mình. Ngay cả khi bạn hoàn toàn chưa có kinh nghiệm, những nội dung Mark cung cấp và truyền đạt sẽ giúp bạn từ một người mới bắt đầu nhanh chóng trở thành chuyên gia công nghệ.

Lời giới thiệu

"Mỗi người hiểu biết cần nắm được thông tin về Bitcoin vì đồng tiền này có thể trở thành phát kiến quan trọng bậc nhất thế giới."

- Leon Luow, ứng cử viên giải Nobel Hòa bình

Bitcoin được gọi là cuộc cách mạng về công nghệ, một cuộc cách mạng có khả năng thay thế ngân hàng, hệ thống thanh toán, chính phủ, vàng, cũng như nhiều loại tiền tệ khác. Nhiều người khác quy nó là lừa đảo, là loại tiền tệ dành cho tội phạm, trào lưu nhất thời hay vài con số không có giá trị nội tại trên máy tính.

Ban đầu, tôi luôn cho rằng Bitcoin là một đồng tiền vô giá trị và cuối cùng sẽ trở nên vô dụng. Vào năm 2013, dường như quan điểm này của tôi về Bitcoin đã đúng, khi nhiều người cho rằng nó chỉ được sử dụng bởi bọn tội phạm buôn bán ma túy trên thị trường giao dịch trực tuyến có tên Silk Road. Cùng năm đó, Silk Road bị đóng cửa và sàn giao dịch Bitcoin lớn nhất Mt. Gox sụp đổ. Khi sàn Mt. Gox đóng cửa, nhiều người liên đới đã bị mất tiền và giá Bitcoin đã giảm hơn 80%.

Sự kiện này dường như đã đặt dấu chấm hết cho Bitcoin, tuy nhiên, từ năm 2013 cho đến thời điểm viết cuốn sách này, Bitcoin đã tăng giá gấp 10 lần, trở thành một hình thức thanh toán và loại tiền tệ được nhiều nơi công nhận là hợp pháp trên thế giới.

Sau nhiều hiểu lầm, tôi đã nghiêm túc dành thời gian tìm hiểu về Bitcoin, tiền mã hóa và công nghệ Blockchain một cách chi tiết. Sau đó, khi thấu hiểu được cách thức hoạt động của Bitcoin và các công nghệ nền tảng đằng sau nó, thái độ của tôi đã thay đổi hẳn, từ việc cho rằng Bitcoin không có bất cứ một tiềm năng hay giá trị sử dụng nào cả, đến việc tin rằng nó có tiềm năng thay đổi cả thế giới.

Lần đầu tiên tìm hiểu về Bitcoin, tôi nhận thấy có rất nhiều thông tin chuyên ngành (nặng tính kỹ thuật) về Bitcoin trên Internet được sắp

xếp lộn xộn và khó hiểu. Tôi nhận ra rằng, chưa có một tài liệu hướng dẫn cụ thể nào giải thích về cách thức Bitcoin hoạt động, cũng như cách sử dụng Bitcoin cho những người chưa có kiến thức chuyên ngành.

Vì vậy, tôi đã viết cuốn sách này vì đây chính là kiểu sách có nội dung, mà vào thời điểm lần đầu tiên tiếp cận và thử tìm hiểu về Bitcoin, tôi muốn đọc.

Mặc dù cuốn sách này sẽ đề cập đến rất nhiều những lợi ích và cách sử dụng Bitcoin, nhưng mục đích chính của nó là cung cấp một cái nhìn toàn diện và những hiểu biết đầy đủ về Bitcoin – cách thức xử lý các rủi ro, những nguy cơ và đồn đại thổi phồng xung quanh Bitcoin.

Nói chung, cuốn sách này được viết cho những người mới tiếp xúc với Bitcoin có nhu cầu tìm kiếm một tài liệu hướng dẫn không nặng tính kỹ thuật để hiểu về đồng tiền này và bắt đầu làm quen với nó. Có một số khía cạnh kỹ thuật được đề cập đến trong cuốn sách, tuy nhiên, chúng sẽ được giải thích dễ hiểu cho những người mới tiếp xúc với Bitcoin.

Tôi hi vọng bạn thích cuốn sách này và thấy nó hữu ích, mang tính giáo dục và làm giàu thêm những kiến thức hiểu biết của bạn về Bitcoin.

Lưu ý: Trong cuốn sách này, từ “Bitcoin” được sử dụng với chữ cái đầu viết hoa “B”, và từ “bitcoin” được sử dụng với chữ cái đầu viết thường “b”.

“Bitcoin” với chữ “B” viết hoa được sử dụng để chỉ mạng lưới Bitcoin, các giao thức hoặc phần mềm, còn “bitcoin” với chữ “b” viết thường để chỉ đồng tiền, ví dụ: “Gửi 2 bitcoin”.

Thuật ngữ “tiền pháp định” (Fiat currency) được sử dụng xuyên suốt cuốn sách này, các loại tiền pháp định là tiền truyền thống, được chính phủ phát hành như đồng đô la Mỹ hay đồng euro.

Chương 1Bitcoin là gì?

“Bitcoin là phát minh quan trọng nhất lịch sử thế giới kể từ khi Internet ra đời.”

- Roger Ver, nhà đầu tư, triệu phú Bitcoin

Trong chương này, chúng ta sẽ tìm hiểu Bitcoin là gì, đồng thời giải đáp một số thắc mắc phổ biến về Bitcoin. Lưu ý, chương này sẽ không đi sâu vào cách thức chính xác Bitcoin hoạt động như thế nào, nội dung này sẽ được đề cập đến trong chương 4 (Cách thức hoạt động của Bitcoin).

Bitcoin là gì?

Bitcoin là một mạng lưới tiền mã hóa; đồng tiền này có thể được dùng để thanh toán điện tử trong các giao dịch mua bán hàng hóa và dịch vụ tương tự các loại tiền truyền thống khác như đồng đô la Mỹ hay đồng euro.

Tuy nhiên, không giống như các loại tiền tệ khác, Bitcoin không được tạo ra hay được kiểm soát bởi chính quyền trung ương. Bitcoin mang đặc tính phi tập trung, có nghĩa là nó không chịu sự kiểm soát của ngân hàng trung ương, chính phủ, công ty hay tổ chức nào.

Bitcoin được chuyển trực tiếp từ người này sang người khác mà không cần sự tham gia của các ngân hàng hay các trung gian tài chính. Những đồng bitcoin được tạo ra và được chuyển giao bởi một mạng lưới gồm hàng ngàn máy tính có kết nối với mạng Bitcoin trên khắp thế giới. Đặc biệt, bitcoin có thể được gửi qua Internet tới người khác giống như gửi email. Ngày nay, chúng ta không còn phải lo nghĩ việc gửi email quốc tế nữa vì chẳng khác gì so với hình thức gửi email cho ai đó cùng văn phòng. Giờ đây, khi Bitcoin dần trở nên phổ biến, việc chuyển tiền quốc tế chẳng khác nào một giao dịch chuyển tiền tại địa phương.

Tiền mã hóa là gì?

Một trong những công nghệ nền tảng của Bitcoin là mật mã học, bao gồm việc mã hóa các thông điệp hoặc thông tin bằng các đoạn mã, do đó những thông tin truyền tải sẽ được ẩn với tất cả mọi người, ngoại trừ những người có quyền truy cập.

Bitcoin được biết đến như là đồng tiền mã hóa (cryptocurrency) đầu tiên được chấp nhận trên toàn cầu, từ “cryptocurrency” là sự kết hợp của từ “cryptography” (mật mã) và “currency” (tiền tệ). Nhìn chung, tầm quan trọng của mật mã học trong cách thức Bitcoin hoạt động sẽ được giải thích ở phần sau trong cuốn sách.

Ai tạo ra Bitcoin?

Bitcoin được tạo ra bởi một lập trình viên hoặc một nhóm người ẩn danh, được biết đến với cái tên là Satoshi Nakamoto. Hiện nay, danh tính thực sự của Satoshi Nakamoto vẫn chưa được biết đến.

Sự xuất hiện của Bitcoin dựa trên một công trình nghiên cứu trước đây về mật mã học và tiền điện tử. Cụ thể, vào năm 2009, Satoshi Nakamoto đã cho xuất bản một chuyên luận nhan đề Bicoin: A Peer-to-Peer Electronic Cash System (tạm dịch: Bitcoin: Hệ thống tiền điện tử ngang cấp).

Bitcoin được tạo ra với vai trò một đồng tiền điện tử với đầy đủ chức năng và một hệ thống thanh toán dựa trên nền tảng về toán học và mật mã học. Bitcoin được thiết kế để không bị kiểm soát bởi bất kỳ cơ quan chính phủ, ngân hàng hay cơ quan trung ương nào cả.

Ai kiểm soát Bitcoin?

Trước hết, phải nói rằng, Bitcoin không bị kiểm soát bởi bất cứ tổ chức nào. Các lập trình viên máy tính tới từ khắp nơi trên thế giới làm việc cùng nhau trong mạng lưới Bitcoin, tuy nhiên, các quyết định về việc thay đổi điều gì đó đều do toàn bộ mạng lưới quyết định. Bên cạnh đó, mọi người từ khắp nơi trên thế giới đóng góp

công suất tính toán của họ vào quá trình xử lý giao dịch trên mạng lưới Bitcoin.

Nhìn chung, các giao dịch được xử lý và được tạo thành bởi phần lớn các thành viên trong mạng lưới. Điều này gần như khiến cho không có bất cứ một cá nhân hay một tổ chức nào có thể thao túng các giao dịch, bởi vì các giao dịch phải được xác nhận bởi phần lớn các thành viên trong mạng lưới. Sự giám sát của nhóm này giữ cho mạng lưới luôn bảo mật và an toàn đồng thời kiểm soát các giao dịch diễn ra.

Đặc biệt, để có thể xâm nhập trái phép và giành quyền kiểm soát mạng lưới Bitcoin, phải kiểm soát được đồng thời hơn 50% số máy tính. Điều này đòi hỏi lực lượng tội phạm phải tấn công hàng ngàn máy tính cùng một lúc, và việc này hầu như không thể thực hiện được với quy mô hiện tại của mạng lưới Bitcoin.

Bên cạnh đó, mã Bitcoin là mã nguồn mở, vì vậy mọi người đều có thể quan sát và thực hiện những thay đổi mang tính chất cải tiến đối với Bitcoin. Khi một sự thay đổi được đề xuất, thì đề xuất này sẽ được gửi đến toàn mạng lưới Bitcoin. Tiếp theo, các máy tính có kết nối với mạng lưới Bitcoin sẽ thực hiện hoạt động bỏ phiếu chấp thuận hay từ chối sự thay đổi đó. Nếu đa số ủng hộ thì sự thay đổi sẽ được thực hiện bởi các lập trình viên.

Một khi sự thay đổi được thực thi, một phiên bản mới của phần mềm Bitcoin được hình thành. Những người đã kết nối với mạng Bitcoin có thể quyết định nâng cấp phần mềm hoặc giữ lại phiên bản cũ. Nếu có một số lượng đủ lớn những người trên mạng lưới thực hiện nâng cấp phiên bản phần mềm Bitcoin, thì sự thay đổi đó sẽ được chấp nhận bởi phần lớn các thành viên trong mạng lưới.

Lưu ý, có thể xảy ra hiện tượng mạng lưới bị chia tách do khác biệt quan điểm về sự thay đổi trên phần mềm, trong đó một phần mạng lưới đồng ý thay đổi và nâng cấp phần mềm nhưng một phần khác kiên trì giữ phiên bản cũ. Nếu có đủ số người tách ra từ mạng lưới chính, thì điều này có thể dẫn đến sự xuất hiện đồng thời hai phiên bản khác nhau của Bitcoin cùng với hai loại tiền tệ riêng biệt. Đây

được gọi là phân nhánh cứng, khái niệm này sẽ được trình bày cụ thể trong phần sau của cuốn sách.

Phi tập trung là gì?

Hiện nay, khi bạn thực hiện một giao dịch, bạn sẽ phải nhờ đến một ngân hàng hay một tổ chức trung gian tài chính.

Tiền trong tài khoản ngân hàng của bạn được ngân hàng giữ. Ngân hàng sẽ kiểm soát tiền của bạn, và tính phí đối với số tiền đó.

Trong khi đó, Paypal không phải ngân hàng, nó vừa là một trung gian tài chính, vừa là một mạng lưới thanh toán. Paypal sẽ tính phí và giữ tiền hộ bạn, chức năng giống như một tài khoản ngân hàng.

Chúng ta tin tưởng gửi tiền tiết kiệm vào các ngân hàng và trung gian tài chính. Chúng ta tin tưởng rằng những tổ chức ấy an toàn, chịu sự kiểm soát của pháp luật và sẽ không xảy ra chuyện bị sụp đổ hay trộm mất tiền của chúng ta. Chúng ta cũng tin rằng danh tính của chúng ta là những thông tin cá nhân được bảo mật và luôn an toàn.

Sự tin tưởng đó của chúng ta thường đi kèm với mức phí giao dịch cao tùy theo tình hình biến động của ngân hàng hay tổ chức tài chính. Cụ thể, ở những nước có hệ thống tài chính và pháp luật đã phát triển và ổn định, bạn có thể chỉ phải trả một khoản phí nhỏ để đổi lấy sự đảm bảo an toàn cho việc bạn tin tưởng vào một tổ chức tài chính lớn khi đặt tiền tại đó.

Tuy nhiên, đối với hàng tỷ người trên thế giới, họ không thể tin tưởng vào ngân hàng, chính phủ hay hệ thống pháp luật sở tại. Họ không có niềm tin đối với các tổ chức theo mô hình tập trung hoặc các hệ thống pháp luật trong việc bảo vệ họ. Hơn nữa, nguy cơ xảy ra những hành vi phạm pháp cũng có thể khiến cho hoạt động giao dịch trực tiếp giữa mọi người gặp rủi ro. Và tại những quốc gia xảy ra tình trạng này, Bitcoin cho phép mọi người giữ tiền của họ ở những nơi nằm ngoài sự kiểm soát của các hệ thống theo mô hình tập trung, và cho phép mọi người giao dịch trực tiếp với nhau, cộng

thêm độ rủi ro thấp hơn so với giao dịch bằng vàng, đá quý hay tiền mặt.

Mạng lưới Bitcoin không có trung gian tài chính. Những khoản tiền được chuyển trên mạng lưới trực tiếp từ người này sang người khác. Chúng được truyền gửi qua mạng lưới Bitcoin, nhưng mạng lưới Bitcoin không bị kiểm soát bởi bất cứ tổ chức nào. Mạng lưới Bitcoin bao gồm hàng ngàn máy tính trên thế giới làm việc cùng nhau để xử lý và lập hồ sơ giao dịch trên Blockchain của Bitcoin.

Trong trường hợp của trung gian tài chính, ví dụ, nếu ai đó tấn công Paypal, kẻ đó có thể truy cập dữ liệu và tiền của tất cả các khách hàng của Paypal. Trong khi đó, tính chất phi tập trung của mạng lưới Bitcoin đồng nghĩa với việc không tồn tại máy chủ trung tâm hay cơ sở dữ liệu nào cả. Theo đó, để kiểm soát được toàn bộ mạng lưới, một kẻ tấn công sẽ phải kiểm soát đồng thời hơn 50% số máy tính trong mạng lưới Bitcoin cùng một lúc.

Thêm vào đó, việc thao túng một giao dịch trên sổ cái Bitcoin phi tập trung là gần như không thể. Bởi vì, các giao dịch, liên tục được kiểm tra và đối chiếu với tất cả các giao dịch, được gửi đến hàng ngàn máy tính để xác nhận tính hợp lệ. Với những hệ thống theo mô hình tập trung, người ta sẽ phải dựa vào một tổ chức trung gian để thực hiện hoạt động kiểm nhận này. Trong khi đó, cấu trúc phi tập trung của Bitcoin đồng nghĩa với hàng ngàn chiếc máy tính sẽ thực thi hoạt động kiểm nhận này để xác thực tính hợp lệ của giao dịch giữa mọi người với nhau.

Với những trung gian tài chính truyền thống, các tài khoản ngân hàng có thể bị đóng băng, tài sản có thể bị tịch thu và việc chuyển tiền có thể bị hạn chế. Trong khi đó, đặc điểm phi tập trung đồng nghĩa với việc chính phủ hay các tổ chức tài chính không thể kiểm soát hay nắm giữ các khoản tiền của bạn. Đặc biệt, trong trường hợp một máy tính trên mạng lưới Bitcoin ngừng hoạt động, thì vẫn còn hàng ngàn máy tính sở hữu một bản sao chuẩn xác của Blockchain Bitcoin tiếp tục hoạt động.

Blockchain là gì?

Blockchain là một sổ cái chung gồm toàn bộ các giao dịch tài chính diễn ra trong mạng lưới Bitcoin.

Blockchain đầu tiên được tạo ra trong mã máy tính gốc cho Bitcoin.

Khi một giao dịch diễn ra trên mạng lưới Bitcoin, nó được tập hợp cùng với các giao dịch khác vào một khối. Khối này được liên kết với các khối trước đó trên Blockchain Bitcoin thông qua quá trình được gọi là "khai thác". Khi một khối các giao dịch được thêm vào, nó được liên kết với khối liền trước trên Blockchain, khối liền trước đó lại được liên kết với khối trước nó nữa.

Các khối được liên kết với nhau, nhờ ứng dụng mật mã học, cho nên các giao dịch, dữ liệu, và thứ tự các khối không thể bị sửa đổi hoặc xóa bỏ. Các khối được liên kết với nhau thành một chuỗi các khối, từ đó hình thành tên gọi Blockchain.

Bạn có thể để ý rằng khi bạn chuyển tiền giữa các ngân hàng, tiền sẽ được lấy ra khỏi tài khoản của bạn, nhưng không xuất hiện trong tài khoản ngân hàng khác cho đến vài ngày sau đó. Nguyên nhân là vì mỗi ngân hàng lưu giữ các sổ cái riêng rẽ, nên họ phải thực hiện hoạt động đối chiếu riêng cho từng tài khoản.

Trong khi đó, Blockchain Bitcoin là sổ cái chung bao gồm toàn bộ các giao dịch. Khi bitcoin được gửi từ người này sang người khác, giao dịch này sẽ được đối chiếu trên cùng một cuốn sổ cái mà mọi người đều có quyền truy cập. Điều này đồng nghĩa với việc giao dịch sẽ xảy ra gần như là ngay lập tức, bởi vì việc gửi và nhận bitcoin được xử lý đồng thời trên cùng một sổ cái.

Khi một giao dịch được tạo ra, nó được gửi đến tất cả các máy tính có kết nối với mạng lưới Bitcoin, các máy tính sẽ xác nhận tính hợp lệ của các giao dịch này, đồng thời nhóm chúng lại thành các khối và thêm vào Blockchain của Bitcoin. Khi một khối các giao dịch được thêm vào, nó được cập nhật trên sổ cái công khai mà tất cả các máy tính trong mạng lưới đều có quyền truy cập và xác thực.

Tất cả mọi người trên mạng lưới Bitcoin đều có thể quan sát các giao dịch từ mới nhất cho đến đầu tiên. Tính minh bạch rất cao của mạng lưới Bitcoin còn góp phần ngăn chặn hoạt động gian lận xảy ra. Bởi vì tất cả mọi người trong mạng lưới đều có thể quan sát tất cả các giao dịch và các số dư tài khoản, cho nên rất dễ dàng kiểm chứng xem các giao dịch có đảm bảo tính hợp lệ hay không.

Hơn nữa, khi một giao dịch diễn ra trên mạng lưới Bitcoin, nó sẽ được ghi chép lại và không thể sửa đổi hay xóa bỏ. Điều này tạo nên một hồ sơ lưu trữ vĩnh viễn cho mọi giao dịch từng xảy ra, cùng với một lịch sử hoạt động truy dẫn tới nguồn gốc của các đồng bitcoin.

Một khối các giao dịch mới được thêm vào Blockchain của Bitcoin cứ 10 phút một lần.

Sự khác nhau giữa Blockchain và Bitcoin là gì?

Thường xảy ra tình trạng nhầm lẫn về sự khác biệt giữa Blockchain và Bitcoin, đặc biệt khi mạng lưới Bitcoin tạo ra Blockchain đầu tiên.

Trước hết, phải nói rằng, Bitcoin là một trường hợp điển hình đầu tiên về một Blockchain hiệu quả, vì vậy trong nhiều năm, cả hai không thể tách rời nhau vì bạn không thể đề cập đến Blockchain mà không nhắc tới Bitcoin. Hơn nữa, Blockchain được cho là công nghệ duy nhất làm nền tảng phía sau Bitcoin, tuy nhiên, trên thực tế, có một loạt các công nghệ đa dạng phối hợp với nhau có liên kết với mạng lưới Bitcoin và Blockchain của Bitcoin.

Mạng lưới Bitcoin chủ yếu được sử dụng cho các giao dịch tài chính, và những giao dịch này được lưu trữ hồ sơ trên Blockchain Bitcoin. Nhưng Blockchain được sử dụng trong mạng lưới Bitcoin chỉ là một ví dụ về cách ứng dụng công nghệ Blockchain.

Hơn nữa, với Bitcoin, mỗi khối được thêm vào Blockchain chứa một nhóm các giao dịch tài chính, tuy nhiên, Blockchain có thể lưu trữ hầu hết mọi loại giao dịch hoặc dữ liệu.

Hiện nay, có hàng loạt phương án ứng dụng tiềm năng đang được khám phá cho các hệ thống dựa trên nền tảng công nghệ Blockchain. Blockchain Bitcoin chỉ lưu trữ các giao dịch tài chính, và hiện vẫn chưa có kế hoạch sử dụng cho bất cứ thứ gì ngoài hoạt động thanh toán kỹ thuật số.

Khai thác Bitcoin là gì?

Khai thác là quá trình thêm các khối giao dịch vào Blockchain Bitcoin để đổi lấy một khoản thanh toán bằng bitcoin.

Bitcoin được tạo ra như thế nào?

Khi một khối mới được thêm vào Blockchain Bitcoin, bitcoin mới được tạo ra dưới hình thức phần thưởng được trả cho người khai thác.

Những bitcoin mới chỉ được tạo ra thông qua quá trình khai thác.

Quá trình tạo ra các đồng bitcoin được đề cập tới trong chương 4 và chương 10.

Liệu bitcoin có thể bị nhân đôi hoặc sao chép như thư điện tử?

Vì những đồng bitcoin chỉ tồn tại dưới dạng điện tử và có thể được truyền gửi như email, cho nên có thể xảy ra trường hợp gửi hai lần cùng một dữ liệu điện tử, giống như cách bạn có thể gửi nhiều email với cùng một nội dung trong nhiều lần. Đây được gọi là giao dịch lặp chi, một vấn đề mà những người nỗ lực tạo ra tiền mã hóa đã phải vật lộn để giải quyết cho đến khi mạng lưới Bitcoin hình thành.

Dù bitcoin chỉ tồn tại dưới hình thức điện tử, và hoạt động truyền gửi bitcoin tương tự như hoạt động gửi thư điện tử, thì chúng cũng không thể bị nhân đôi hay sao chép.

Trong các hệ thống thanh toán truyền thống, sẽ cần một tổ chức trung gian như ngân hàng hay Paypal đảm bảo rằng đồng tiền điện tử sẽ không bị sao chép hay lặp chi. Mạng lưới Bitcoin không có

trung gian, và đa số các thành viên trong mạng lưới phải đồng thuận rằng các giao dịch là hợp lệ.

Nếu bạn gửi bitcoin cho người khác, thì các máy tính trên mạng lưới sẽ kiểm tra xem bạn có quyền gửi số bitcoin đó hay không hoặc chúng đã bị chi tiêu chưa. Nếu chúng đã được chi tiêu, thì giao dịch sẽ bị từ chối.

Bitcoin được lưu trữ ở đâu?

Khi bạn sở hữu bitcoin, chúng được cất giữ trong ví điện tử của bạn. Chiếc ví này không thực sự chứa bitcoin nhưng lại chứa khóa công khai và khóa cá nhân được dùng để truy cập và chuyển giao bitcoin.

Ví điện tử chứa những địa chỉ Bitcoin mà từ đó bạn có quyền nhận được bitcoin. Cách thức lập ví Bitcoin sẽ được đề cập chi tiết trong nội dung của cuốn sách.

Bitcoin có ẩn danh không?

Có, Bitcoin được thiết kế gần như là ẩn danh. Mọi giao dịch mà bạn thực hiện trên mạng lưới Bitcoin sẽ không hiển thị danh tính hay bất kỳ thông tin cá nhân nào của bạn.

Tuy nhiên, nếu bạn mua bitcoin bằng các loại tiền tệ như đồng đô la Mỹ, bạn sẽ phải thiết lập tài khoản với một công ty được kiểm soát bởi hệ thống pháp luật tương tự như với các tổ chức tài chính khác.

Các quy định pháp luật này đòi hỏi bạn xác thực danh tính trong quá trình khởi tạo tài khoản và mua bitcoin bằng các phương thức thanh toán truyền thống.

Trong trường hợp bạn mua bitcoin từ một công ty mà tại đó bạn đã xác minh danh tính, thì các giao dịch từ tài khoản này có thể bị công ty liên kết với danh tính của bạn. Các công ty như thế này được kiểm soát bằng các điều luật giống như các tổ chức tài chính, vì vậy nếu bạn mua bitcoin thông qua một công ty có trụ sở đặt tại Mỹ, sau

đó gửi số bitcoin đó đến địa chỉ bitcoin ở Cuba, Iran hoặc các quốc gia khác nơi Mỹ có các định chế tài chính, thì các công ty này sẽ có thể truy nguyên và thậm chí hủy bỏ tài khoản của bạn.

Ngay cả khi ví Bitcoin của bạn hoàn toàn ẩn danh, nếu bạn mua sắm trong một cửa hàng nào đó, chủ sở hữu cửa hàng sẽ có thể xem địa chỉ nguồn gốc mà nó từ đâu đến và liên kết với nhận dạng của bạn.

Bên cạnh đó, có nhiều cách để đảm bảo giao dịch Bitcoin của bạn ẩn danh, chẳng hạn như việc sử dụng các địa chỉ khác nhau và ví khác nhau. Bạn hãy lưu ý rằng, việc này có thể không hoàn toàn ẩn danh, và thậm chí vẫn có thể có những quy định mà bạn phải tuân thủ.

Bitcoin có giống Paypal không?

Không, Paypal là một tổ chức trung gian cho phép bạn dễ dàng truyền gửi tiền tệ truyền thống sang cho người khác, và Paypal hoạt động tương tự như một tài khoản ngân hàng truyền thống với một tổ chức tài chính.

Trong khi bạn có thể gửi tiền cho nhiều người qua Paypal nhờ sử dụng địa chỉ email của họ, thì hoạt động này không hề giống như hoạt động gửi tiền qua mạng lưới Bitcoin. Cụ thể, tiền được chuyển giao qua Paypal là bằng đô la Mỹ, euro và các loại tiền tệ pháp định khác. Ẩn sau đó, những giao dịch này được đối chiếu bằng những sổ cái cá nhân nội bộ, những hệ thống theo mô hình tập trung và các tài khoản ngân hàng truyền thống.

Bitcoin rất khác, bởi vì nó vừa là loại tiền tệ vừa là nhà cung cấp dịch vụ thanh toán hoàn toàn riêng biệt. Nó hoạt động mà không cần sự kiểm soát của chính phủ hay bất kỳ tổ chức trung gian nào để xử lý giao dịch. Bên cạnh đó, các giao dịch được thực hiện bằng bitcoin, được xử lý bởi một mạng lưới phi tập trung gồm hàng ngàn máy tính kết nối với nhau. Tất cả các giao dịch được công bố trong cuốn sổ cái công khai mà mọi người hoàn toàn có thể xem. Ở đây, không có bất kỳ tài khoản ngân hàng truyền thống, kế toán viên hay

các hệ thống theo mô hình tập trung nội bộ nào thực hiện hoạt động lưu giữ bitcoin hay đối chiếu các giao dịch.

Lợi ích của việc sử dụng Bitcoin là gì?

Có rất nhiều lợi ích của việc sử dụng Bitcoin. Rất nhiều trong số những lợi ích này sẽ được đề cập chi tiết trong chương “Lợi ích của Bitcoin”.

Những nguy cơ và bất lợi khi sử dụng Bitcoin là gì?

Những nguy cơ và bất lợi của việc sử dụng Bitcoin được đề cập cụ thể trong chương 6: “Rủi ro và bất lợi của Bitcoin”.

Tổng kết chương 1

Lần đầu tiên trong lịch sử, mọi người không cần phụ thuộc vào đồng tiền và hệ thống tài chính sở tại. Thế giới xuất hiện một loại tiền tệ có thể được sử dụng trên phạm vi toàn cầu, một loại tiền tệ cho phép bất cứ ai cũng có thể thiết lập tài khoản và giao dịch trên mạng lưới, bất kể họ là ai và đang sinh sống ở đâu.

Hiện nay, trên thế giới, số người có điện thoại di động còn nhiều hơn số người có tài khoản ngân hàng. Nhiều người có thể truy cập Internet nhưng không thể mở một tài khoản ngân hàng hoặc đăng ký vay vốn. Nếu không có tài khoản ngân hàng, sẽ có rất hàng ngàn người bị loại ra khỏi hệ thống tài chính mà nhiều người trong chúng ta vẫn coi là hiển nhiên.

Bitcoin không có tỷ giá hối đoái hay phí giao dịch quốc tế đắt đỏ. Bitcoin là loại tiền tệ toàn cầu không bị hạn chế bởi những rào cản chính trị và kinh tế - xã hội.

Trong các chương tiếp theo, chúng ta sẽ khám phá lịch sử của Bitcoin và chi tiết cách thức Bitcoin hoạt động.

Chương 2Tiền là gì?

“Tiền là một thỏa thuận chung. Nếu có đủ số người đi đến một thỏa thuận như vậy thì điều họ đồng thuận sẽ trở thành thứ yếu, cho dù đó là vật nuôi trong trang trại, vàng, kim cương, giấy, hoặc đơn giản chỉ là một đoạn mã.

Lịch sử đã chứng minh rằng tất cả những trường hợp này đều đúng. Một khi chúng ta coi tiền kỹ thuật số là bình thường, ai biết được tương lai đồng tiền sẽ ra sao?”

- S.E. Sever, nhà văn

“Khởi tạo một loại tiền mới thật dễ dàng làm sao, bất cứ ai cũng có thể làm được điều đó. Bí quyết ở đây là, hãy làm cho mọi người chấp nhận nó, bởi việc họ đồng ý sử dụng mới mang lại cho nó giá trị ‘đồng tiền’.“

– Adam B. Levine, giám đốc điều hành Tokenly

Để hiểu tại sao các doanh nghiệp và mọi người chấp nhận Bitcoin với vai trò hình thức thanh toán giống như bất kỳ loại tiền tệ nào khác, trước tiên bạn cần hiểu thị trường tài chính hoạt động như thế nào, và có kiến thức về các hình thái tiền tệ trong lịch sử.

Trong chương này, chúng ta sẽ tìm hiểu sự phát triển của tiền tệ trong suốt chiều dài lịch sử, cùng với một số nguyên tắc cơ bản về tiền tệ, về nền kinh tế và thị trường tài chính. Đây không phải là một bản mô tả lịch sử hoàn chỉnh, mà chỉ là một bức tranh tổng quan để hiểu cách thức Bitcoin hoạt động ra sao.

Tiền tệ trong tiến trình lịch sử

Khi mới hình thành, các xã hội chủ yếu là những nền kinh tế dựa trên việc trao đổi hàng hóa trực tiếp. Các bộ lạc sống gần biển có thể đổi cá lấy thịt với các bộ lạc sống sâu trong đất liền.

Khi các cộng đồng trở nên lớn hơn, hàng loạt các sản phẩm cùng với các dịch vụ đều tăng lên. Càng nhiều sản phẩm xuất hiện trong nền kinh tế, càng khó thực hiện giao dịch, bởi vì sẽ xuất hiện hàng trăm hay hàng ngàn mức trao đổi sản phẩm.

Khoảng 3.000 năm trước Công nguyên, vào thời kỳ của nền văn minh Sumer cổ đại, một phương tiện trao đổi phổ biến đã được tạo ra. Các bình tiêu chuẩn được đưa ra để đo lường số lúa mạch, mỗi bình đều đựng một lượng lúa mạch bằng nhau khi cân lên, và theo đó tất cả hàng hóa và dịch vụ đều được định giá theo trọng lượng của lúa mạch. Công lao động được trả theo số thóc lúa tương ứng, và thóc lúa trở thành đơn vị trao đổi trong xã hội thời Sumer.[1]

Tiếp theo, trong nền văn minh Babylon cổ đại, một trong những bộ luật thành văn cổ xưa nhất là Bộ luật Hammurabi. Bộ luật này định rõ mức lương tối thiểu cho hoạt động thuê nhân công, và hoạt động vay mượn động vật hay dụng cụ cày ruộng. Bên cạnh đó, lương và giá cả chủ yếu được thiết lập dựa theo trọng lượng ngũ cốc.[2]

Các sản phẩm như lúa mì, lúa mạch, và ngô đều dễ bị hư hỏng, ôi thiu, và có thể dễ dàng bị chuột bọ phá hoại. Ngũ cốc còn cần có không gian để cất trữ, khó tích lũy hoặc vận chuyển với số lượng lớn. Hơn nữa, ngũ cốc còn không bảo quản được lâu dài, và chắc chắn không thể được cất trữ cho đến khi bạn nghỉ hưu. Trong khi đó, các kim loại như vàng và bạc, đều là những vật liệu thực hiện chức năng lưu giữ giá trị tốt hơn, chúng có thể dễ dàng tích trữ và cất giữ lâu dài, nên dần dần càng có nhiều người sử dụng chúng làm phương tiện trao đổi.[3]

Khi bạc và vàng bắt đầu được sử dụng như một phương tiện thanh toán, trọng lượng của các kim loại được tính toán dựa theo cân nặng của đá với trọng lượng tiêu chuẩn do nhà vua công bố. Tuy nhiên, hành vi gian lận và lừa đảo dần trở nên phổ biến, các thương nhân sử dụng những viên đá tuy trông giống nhau nhưng lại có mức cân nặng khác nhau, hay chỉnh sửa chiếc cân để thu được nhiều bạc và vàng hơn.

Hành vi gian lận trở nên rất phổ biến đến mức mà Kinh Cựu Ước còn có một số câu thơ bàn về hành vi gian lận cân nặng và độ đo. Một vài ví dụ sau được lấy ra từ Kinh Thánh (bản của Vua James): "Các cân nặng khác nhau và độ đo khác nhau, cả hai đều là những điều đáng ghê tởm trước Chúa"[4] và "Một bàn cân và cái cân tiểu ly đều là những thứ thuộc về Chúa; Toàn bộ trọng lượng của chiếc túi là mối quan tâm của Ngài".[5]

Về sau, tiền xu được nhà vua và chính quyền cho đúc với trọng lượng cố định bằng bạc và vàng đặt trong đó. Đáng chú ý là, các kim loại quý trong tiền xu đều hiếm có, và không thể bị làm giả. Hơn nữa, trọng lượng của vàng hoặc bạc bên trong một đồng tiền xu là một con số xác định – và nó sẽ quyết định giá trị của đồng xu. Việc tạo ra những đồng xu giả bằng kim loại rẻ tiền hơn sẽ bị trừng phạt nghiêm khắc.

Nhìn chung, những đồng tiền xu tiêu chuẩn đã giải quyết rất nhiều trở ngại của việc sử dụng ngũ cốc hoặc kim loại làm tiền. Một trong những loại tiền tệ đầu tiên là "Shekel", bắt nguồn từ ngôn ngữ Akkadian của người Sumer cổ đại, trong đó "she" có nghĩa là lúa mạch và "kel" là "trọng lượng". Một shekel đại diện cho một số lượng lúa mạch nhất định, với hình ảnh lúa mạch được in trên nhiều đồng xu cổ. Người Israel vẫn gọi đồng tiền của mình là Shekel và từ này cũng có nghĩa là "trọng lượng" hoặc "cân nặng" trong tiếng Do Thái.[6]

Trong khi đó, tiền giấy được sử dụng xuyên suốt nền văn minh cổ đại của Trung Quốc và châu Á. Hốt Tất Liệt đã phát hành một loại tiền giấy được chấp thuận lưu thông suốt thời đại Đế chế Mông Cổ. Nhà thám hiểm Marco Polo đã dành thời gian đến thăm Hốt Tất Liệt trong suốt thời kỳ ông trị vì, và trong cuốn The Travels of Marco Polo (tạm dịch: Những chuyến du hành của Marco Polo), ông viết: "Làm thế nào mà Đại Hãn có thể biến vỏ cây thành một thứ giống như giấy, từ đó lưu thông tiền ra khắp đất nước của ông? Tất cả những tờ giấy này được phát hành với sự trang trọng và uy quyền như thể được làm bằng vàng hoặc bạc tinh khiết. Tất cả mọi người đều có thể mang theo dễ dàng; bất cứ nơi đâu trên khắp lãnh thổ

của Đại Hãn, họ đều thấy chúng, và có thể thuận lợi thực hiện tất cả các giao dịch mua bán hàng hóa bằng công cụ này như thể chúng là những đồng xu bằng vàng nguyên chất vậy.”[7]

Vào khoảng thế kỷ 14, những tờ giấy có mệnh giá do các ngân hàng ở Ý phát hành có thể được sử dụng để đổi lấy vàng trong kho dự trữ của họ. Những tờ giấy có giá này còn được dùng để đổi lấy hàng hóa, người nhận có thể đổi nó lấy vàng được ngân hàng cất giữ. Chúng được gọi là “nota di Banco”, cụm từ “giấy bạc ngân hàng” bắt nguồn từ đó và vẫn được sử dụng cho tới ngày nay.

Những tờ giấy có mệnh giá không phải được sử dụng rộng rãi trên thế giới, và tiền xu chỉ là một hình thức của tiền được dùng để trao đổi. Vỏ sò, vỏ trai, và những tấm da hoẵng được sử dụng trên khắp Bắc Mỹ. Chúng đã được coi là phương tiện thanh toán giữa những người bản địa, và người khai hoang thuộc địa chấp nhận như hình thái tiền tệ sơ khai. Rất nhiều cụm từ chỉ tiền bạc ngày nay xuất phát từ việc sử dụng các vật dụng đóng vai trò như tiền thời đó.

Trong số những vật dụng được sử dụng làm tiền, còn có wampum. Về hình thức, wampum là những hạt màu tím hoặc trắng được làm từ vỏ trai hoặc vỏ ốc xoắn. Những chiếc hạt này được đánh bóng và xâu chuỗi làm đồ trang sức hoặc dây đai. Chúng đã được chấp nhận như là một hình thức tiền tệ hợp pháp trên khắp Bắc Mỹ. Học phí một năm học tại Đại học Harvard khoảng 1.900 hạt wampum thời những năm 1700. Đặc biệt, vào thời kỳ đó, một vị chủ tịch của Đại học Harvard phàn nàn rằng kho bạc của trường đại học toàn hạt wampum giả.[8]

Nhìn chung, quãng thời gian từ lúc tiền giấy được tạo ra lần đầu tiên cho đến lúc những tờ giấy có giá được sử dụng phổ biến trên toàn thế giới kéo dài hàng thế kỷ. Và giống như các ngân hàng Ý vào thế kỷ 14, các chính phủ đã phát hành các tờ giấy có giá đại diện cho giá trị của những kim loại mà họ có thể trao đổi. Khi ấy, tiền tệ ở Anh được gọi là bảng (pound), bởi vì ban đầu một tờ tiền có giá một bảng Anh có thể trao đổi tương ứng với một pound* kim loại bạc.

Điều này cũng tương tự như từ “shekel” bắt nguồn từ những từ liên quan đến trọng lượng.

* Đơn vị đo trọng lượng, 01 pound tương đương với khoảng 0,454kg.

Năm 1945, hệ thống Bretton Woods đã được triển khai với hơn 40 quốc gia đồng ý tham gia, trong đó họ chấp thuận việc đồng tiền của họ sẽ được gắn với giá trị của vàng. Tất cả các loại tiền tệ chính của nhiều quốc gia trên thế giới có thể được trao đổi với vàng theo một tỷ giá cố định. Bên cạnh các nguyên do khác, thì việc các đồng tiền đều được đảm bảo bằng vàng, sẽ là một nguyên do khiến chúng trở nên có giá trị, từ đó sẽ giảm thiểu rủi ro và tạo sự ổn định cho tỷ giá trao đổi trong lĩnh vực thương mại quốc tế.

Hệ thống Bretton Woods tiếp tục duy trì cho đến năm 1971 khi Mỹ rút khỏi thỏa thuận và không còn đảm bảo đồng đô la Mỹ theo vàng nữa. Hiện nay, các loại tiền tệ không còn liên kết vàng, kim loại hay một loại hàng hóa khác với giá trị nội tại của chúng nữa. Tức là, mọi người không thể đổi một tờ giấy có giá một bảng Anh để lấy một pound kim loại bạc, và cũng không thể đổi đô la Mỹ để lấy vàng nữa. Về cơ bản, các tờ tiền trong ví của bạn chỉ là những tờ giấy với con số ghi trên đó, vậy tại sao chúng ta chấp nhận tiền như một hình thức có giá trị?

Giá trị của tiền là gì?

Nếu nghĩ về tiền ngày nay, chắc hẳn bạn sẽ nhớ tới những đồng tiền xu, những tờ giấy có mệnh giá và những con số điện tử trong tài khoản. Nếu bạn hỏi mọi người tờ giấy bạc ngân hàng 100 đô la đáng giá bao nhiêu, thì có lẽ họ sẽ cho rằng đó là một câu hỏi quái lạ, và đều cho ra một phản hồi giống nhau: “Tất nhiên là có giá 100 đô la rồi”. Tuy nhiên, nếu bạn viết “tờ giấy này có giá 100 đô la” lên trên một tờ giấy bình thường, và đưa nó cho một người rồi hỏi họ nó đáng giá bao nhiêu, họ chắc chắn sẽ trả lời bạn rằng nó vô giá trị.

Tại sao lại như vậy? Cả hai đều chỉ là những tờ giấy với con số ghi trên đó, nhưng tại sao chúng ta lại nghiễm nhiên tin rằng chỉ một

trong số chúng có giá trị và cái còn lại thì không. Nếu nhìn qua, cả tờ giấy bạc có giá 100 đô la và tờ giấy bình thường với dòng chữ viết tay “100 đô la” trên đó, đều gần như giống nhau, với cùng chất liệu và cùng con số. Chúng có cùng những ứng dụng thực tế, bạn có thể đốt để giữ ấm, bạn có thể viết lên chúng, cả hai đều có cùng độ bền, trọng lượng và kích cỡ. Nhìn chung, không có sự khác biệt mấy trong cấu trúc vật lý của một tờ giấy bạc ngân hàng và một tờ giấy bình thường với con số được viết lên đó.

Sự khác biệt ở đây chính là nhận thức và lòng tin. Bạn tin rằng nếu bạn chấp nhận tờ giấy bạc ngân hàng do chính phủ cấp, bạn có thể vào cửa hàng và đổi nó để lấy các sản phẩm hoặc dịch vụ khác. Hơn nữa, nếu vào cửa hàng, bạn có niềm tin rằng chủ cửa hàng sẽ chấp nhận tờ giấy bạc đó, và cứ thế, giống như việc chủ cửa hàng tin rằng nếu họ chấp nhận tờ giấy bạc đó, họ có thể trao đổi tờ giấy đó một lần nữa để lấy các mặt hàng khác.

Bạn của bạn có thể chấp nhận một tờ giấy cam kết với dòng chữ viết tay “Tôi nợ bạn 100 đô la” để đổi lấy việc bán cho bạn một món hàng, và tin tưởng rằng họ có thể mang mảnh giấy đó đến gặp bạn vào một ngày nào đó, và đổi lại với giá trị 100 đô la. Tuy nhiên, họ không thể cầm nó vào một cửa hàng để trao đổi lấy hàng hóa, và chủ cửa hàng ở đó sẽ không tin họ có thể thực hiện trao đổi tờ giấy đó một lần nữa để lấy giá trị 100 đô la.

Tương tự, những tờ tiền chỉ là những tờ giấy với dòng cam kết “Tôi nợ bạn” của chính phủ, và nó cung cấp cho mọi người một niềm tin rằng nó có thể được trao đổi và sẽ được người khác chấp nhận. Mọi người cũng tin tưởng rằng tiền không dễ bị làm giả, và nếu những tờ tiền giả được tạo ra, những kẻ làm nên chúng sẽ bị trừng trị theo pháp luật.

Phần lớn nguồn cung tiền của thế giới không tồn tại dưới hình thức tiền xu hoặc tờ giấy bạc. Nếu ngày mai tất cả mọi người vào ngân hàng để rút tiền, thì ngân hàng sẽ không có đủ tiền cho tất cả mọi người. Kịch bản này đã xảy ra gần đây ở Hy Lạp khi chính phủ và ngân hàng đặt ra định mức số tiền mọi người có thể rút ra mỗi ngày.

Chúng ta đều biết rằng số tiền này chỉ tồn tại dưới hình thức điện tử, và không có đồng tiền xu, tiền kim loại hay vàng nào bảo đảm, vậy tại sao chúng ta chấp nhận nó?

Nếu tôi gửi một email với nội dung có dòng chữ đánh máy “1.000 đô la”, thì tại sao những chữ số điện tử này không có cùng giá trị với những chữ số điện tử xuất hiện trong tài khoản của bạn?

Giống như tiền xu và tờ giấy bạc, chúng ta tin rằng chúng ta có thể chuyển những con số điện tử trong tài khoản ngân hàng cho các cá nhân và doanh nghiệp, để đổi lấy hàng hóa và dịch vụ. Trong khi đó, con số được viết trong nội dung email có thể bị sao chép dễ dàng, và bất cứ ai cũng có thể viết số vào email và gửi đi càng nhiều email càng tốt. Điều này khiến những chữ số điện tử trong email không có giá trị như một hình thức thanh toán, bởi vì mọi người sẽ không chấp nhận chúng.

Còn đối với hình thức tiền điện tử trong tài khoản ngân hàng, chúng ta tin tưởng rằng các ngân hàng đang lưu giữ những hồ sơ chính xác tất cả những số dư tài khoản cũng như những khoản tiền được chuyển đi, và số liệu điện tử đó không thể bị sao chép như khi xuất hiện trong email.

Mặc dù những con số điện tử đó đại diện cho rất nhiều tiền, nhưng cũng chỉ là con số điện tử được viết trên máy tính. Chúng có giá trị bởi vì chúng ta tin tưởng vào các ngân hàng, chính phủ và các tổ chức tài chính trong việc lưu giữ hồ sơ về số tiền của chúng ta, cũng như người khác chấp nhận chúng như một hình thức thanh toán.

Ghi chú

Những nội dung trên chính là điểm cốt lõi sẽ hỗ trợ để trả lời cho câu hỏi “Tại sao Bitcoin lại có giá trị như một loại tiền tệ?” Ban đầu, tôi đã nghĩ rằng tiền tệ kỹ thuật số không do chính phủ ban hành sẽ chẳng có giá trị nào hết.

Vào thời điểm lạc quan nhất, tôi nghĩ rằng Bitcoin có cùng giá trị như loại tiền tệ được phát hành bởi một quốc gia như Zimbabwe. Cụ thể hơn, tại Zimbabwe, tiền tệ do chính phủ phát hành chỉ có thể được sử dụng trong phạm vi nội địa, và thậm chí nhiều cửa hàng còn từ chối coi nó như là một phương thức thanh toán. Ở đất nước này, bạn sẽ phải mang theo các xe cút kít chất đầy tiền giấy chỉ để mua những đồ tạp phẩm cơ bản, và những tờ giấy bạc có giá trị lên đến hàng nghìn tỷ đô la đã được phát hành do giá trị của đồng tiền sụt giảm vô cùng.

Ngay khi hiểu được cách thức Bitcoin hoạt động để ngăn chặn tình trạng bitcoin bị sao chép, tôi đã thấy được giá trị và sự kỳ diệu trong Bitcoin. Chúng ta sẽ xem xét nội dung này cụ thể hơn trong chương bàn về cách thức hoạt động của Bitcoin.

Tại sao Bitcoin có giá trị?

"Các nhà kinh tế học và các nhà báo thường bị cuốn vào câu hỏi: Tại sao Bitcoin lại có giá trị? Đáp án rất đơn giản. Bởi vì nó hữu ích và có tính khan hiếm."

- Erik Voorhees, giám đốc điều hành ShapeShift

Về cơ bản, nếu mọi người chấp nhận thứ gì đó như một hình thức thanh toán, nó sẽ có giá trị. Đồng tiền có giá trị trong hệ thống mà chúng được chấp nhận; nếu không được bất cứ ai thừa nhận sử dụng để trao đổi lấy hàng hóa hoặc dịch vụ, thì chúng bị coi là giá trị trong hệ thống đó.

Ví dụ, đồng đô la Canada được chấp nhận thanh toán tại Starbucks ở Canada, nhưng bạn không thể mang đồng đô la Canada đến Mỹ và chi tiêu chúng ở quán Starbucks tại Mỹ được. Những tờ giấy bạc giống nhau sẽ được sử dụng trong cùng một cộng đồng, nên bạn phải đổi đồng đô la Canada thành đồng đô la Mỹ để mua hàng tại Mỹ trước đã.

Hơn nữa, những thứ được coi là tiền cũng có thể thay đổi trong một hệ thống. Trước đây, Harvard chấp nhận hạt wampum như một hình

thức thanh toán học phí, thì ngày nay, không có khả năng họ cho phép chi trả học phí bằng wampum.

Vì vậy, Bitcoin có giá trị bởi mọi người chấp nhận nó như một hình thức thanh toán. Đôi lúc, bạn có thể muốn mua hàng hóa hay dịch vụ trực tuyến mà tại đó Bitcoin là phương thức thanh toán được chấp nhận, nhưng bạn lại chỉ có đồng đô la Mỹ trong tay. Để mua hàng thành công trong trường hợp này, bạn cần đổi đồng đô la Mỹ sang bitcoin, sau đó mua hàng bằng bitcoin.

Khi trao đổi đô la Mỹ với bitcoin, bạn đang tạo ra nhu cầu cho bitcoin, đồng thời tham gia vào việc mua chúng từ nguồn cung bitcoin hiện thời. Một trong những bài học đầu tiên được giảng dạy trong lớp học kinh tế là lý thuyết cung-cầu. Đây là yếu tố chính sẽ quyết định giá trị của bitcoin.

Cung và cầu

• Kinh tế học dạy chúng ta rằng khi nhu cầu về một mặt hàng tăng lên, giá của mặt hàng đó sẽ tăng lên, nhưng nếu nhu cầu giảm xuống thì giá của nó sẽ giảm xuống.

• Về phía cung, nếu nguồn cung một mặt hàng tăng lên, giá của mặt hàng đó sẽ giảm đi do nhiều hàng hóa sẵn có hơn.

• Tuy nhiên, nếu nguồn cung của một mặt hàng giảm, giá của mặt hàng đó sẽ tăng do có hàng hóa sẵn có hơn.

Chỉ có đúng 21 triệu bitcoin sẽ được tạo ra, điều này làm số lượng bitcoin trở nên hạn chế. Chính vì bị giới hạn, cho nên giá trị của bitcoin gia tăng khi có nhiều người mua chúng hơn, và giảm xuống nếu nhiều người bán chúng.

Về lý thuyết, càng nhiều cửa hàng chấp nhận Bitcoin như một hình thức thanh toán, thì nhu cầu đối với bitcoin sẽ ngày càng cao, tức là giá của chúng sẽ trở nên cao hơn. Tương tự như vậy, nếu ngày càng ít cửa hàng chấp nhận chúng như một hình thức thanh toán,

nhu cầu đối với bitcoin sẽ ngày càng thấp hơn, đồng nghĩa với giá của chúng sẽ giảm xuống.

Chỉ có một số bitcoin hữu hạn là một yếu tố rất quan trọng. Về phía cung, chúng ta không thể tạo ra quá 21 triệu bitcoin. Nguồn cung bitcoin hạn chế đồng nghĩa với việc sẽ không xảy ra tình trạng dư thừa bitcoin – một điều có thể dẫn đến việc sụt giảm giá trị của chúng.

Nếu xem xét trường hợp của đồng đô la Zimbabwe trong 20 năm qua, chúng ta sẽ thấy rằng: Chính phủ không có đủ tiền để trả nợ và thanh toán các khoản nợ và chi phí, vì vậy chính phủ quyết định in thêm tiền. Mỗi lần như thế, nguồn cung tiền lại tăng, từ đó làm giảm giá trị của đồng tiền. Và một khi giá trị của đồng tiền giảm xuống, chính phủ lại phải in thêm tiền. Điều này dẫn đến hiện tượng siêu lạm phát với chu kỳ in thêm tiền liên tục, hạ thấp hơn nữa giá trị của đồng tiền và khiến chính phủ phải in nhiều tiền hơn nữa.

Vào năm 2015, đồng đô la Zimbabwe bị mất giá nhiều đến nỗi 200 nghìn tỷ đô la Zimbabwe có giá trị chưa tới 1 đô la Mỹ. Zimbabwe cuối cùng tuyên bố rằng đồng tiền của họ đã vô giá trị, và chấp nhận sử dụng 8 loại tiền tệ lớn làm phương tiện trao đổi hợp pháp trong nước bao gồm đồng đô la Mỹ, đồng rand Nam Phi, đồng pula của Botswanan, đồng bảng Anh, đồng đô la Úc, đồng Nhân dân tệ, đồng rupee Ấn Độ và đồng yên Nhật.

Lòng tin

Thậm chí trước khi đồng đô la Zimbabwe bị tuyên bố là vô giá trị, bị bãi bỏ và được thay bằng các loại tiền tệ quốc tế khác, thì đồng tiền này đã không được chấp nhận tại nhiều nơi ngay trong đất nước Zimbabwe. Các chủ cửa hàng không muốn coi nó là phương thức thanh toán, mọi người đều mất lòng tin về việc nó sẽ được đông đảo chấp nhận, kết quả là, người dân Zimbabwe bán bất cứ đồng đô la Zimbabwe nào mà họ có, để đổi lấy các loại tiền tệ khác hoặc kim loại quý.

Việc chấp nhận một loại tiền tệ gắn bó mật thiết với sự tin tưởng vào loại tiền tệ đó. Nếu người ta có niềm tin rằng đồng tiền sẽ trở nên ổn định và giữ được giá trị của nó, họ sẽ chấp nhận nó để đổi lấy các mặt hàng khác. Ví dụ, niềm tin và sự ổn định của đồng bảng Anh đã được tạo ra khi mọi người biết rằng họ có thể đổi 1 pound kim loại bạc để lấy một tờ giấy bạc trị giá 1 bảng Anh. Tiêu chuẩn về vàng của hệ thống Bretton Woods cũng quy định tương tự đối với các loại tiền tệ quốc tế, khi mà mọi người đều biết rằng mỗi tờ tiền đều có thể dùng để đổi lấy một lượng kim loại vàng nhất định.

Nhiều loại tiền tệ hiện đại không có kim loại quý đứng sau đảm bảo cho chúng. Và niềm tin rất khó giành được nhưng lại rất dễ mất đi, đặc biệt khi các quốc gia bắt đầu in nhiều tiền quá mức. Mỗi tờ giấy bạc chỉ có giá trị khi ở đó mọi người tin rằng nó có. Giá trị này dựa trên niềm tin rằng đồng tiền sẽ duy trì được giá trị của nó, và được chấp nhận như một phương tiện trao đổi.

Zimbabwe chỉ là một trong nhiều quốc gia trên thế giới nơi người ta không tin tưởng vào đồng tiền của họ. Năm 2000, Ecuador đã bãi bỏ đồng tiền của mình và cho phép lưu thông đồng đô la Mỹ như một phương tiện trao đổi. Nhiều quốc gia khác từ châu Phi, Mỹ Latinh tới châu Á như Campuchia, Việt Nam, Myanmar, Venezuela, Nicaragua, Cuba, Liberia đều chấp nhận đồng đô la Mỹ, nhưng vẫn ưu tiên đồng tiền địa phương trong các giao dịch trao đổi.

Tại nhiều quốc gia sở hữu đồng tiền riêng, đồng nội tệ có thể không được chấp nhận hoặc được sử dụng rộng rãi, chẳng hạn như máy ATM ở Campuchia sẽ nhả đô la Mỹ chứ không phải nội tệ. Toàn bộ giá cả ở Campuchia đều được hiển thị bằng đô la Mỹ, và các giao dịch cũng được thực hiện bằng đồng đô la Mỹ. Đồng tiền quốc nội riel của Campuchia được sử dụng chủ yếu như tiền lẻ để thay cho những mệnh giá nhỏ dưới 1 đô la Mỹ.

Người Campuchia, giống như nhiều dân tộc khác trên thế giới, không tin rằng đồng tiền địa phương của họ là nơi cất trữ giá trị đáng tin cậy. Họ sử dụng đồng nội tệ cho các giao dịch nhỏ, nhưng đối với các giao dịch lớn, đồng đô la Mỹ được xem là nơi cất trữ giá trị ổn định và đáng tin cậy hơn.

Cất trữ giá trị

Được xem như nơi cất trữ giá trị đáng tin cậy là đặc điểm quan trọng khác của một đồng tiền ổn định. Chẳng hạn, nếu bạn bán hàng hóa và nhận về khoản tiền 100 đô la, thì tờ giấy bạc đó cất trữ giá trị cho đến khi nó được trao đổi với mức giá 100 đô la của những mặt hàng hoặc dịch vụ trong một giao dịch khác.

Hầu như mọi thứ đều có thể trở thành một nơi cất trữ giá trị, tuy nhiên độ tin cậy của giá trị sẽ có sự khác nhau đáng kể. Như đã đề cập trước đó, lúa mạch, lúa mì, ngũ cốc và thịt đã từng được sử dụng để trao đổi giá trị. Tuy nhiên, chúng chưa bao giờ là một nơi cất trữ giá trị đáng tin cậy, bởi vì chúng dễ hư hỏng và tốn nhiều không gian bảo quản.

Các mặt hàng như rượu Rum trở thành nơi cất trữ giá trị có mức độ đáng tin cậy cao hơn, vì có tuổi thọ lâu dài hơn rất nhiều so với ngũ cốc hay thịt. Rượu Rum có thể được cất trữ trong một khoảng thời gian dài những vẫn giữ được giá trị của nó. Trong suốt 25 năm đầu khai thác thuộc địa tại Úc, không một loại tiền tệ nào có thể được tạo ra dễ dàng, nên rượu Rum được sử dụng như một đồng tiền để trao đổi. Lương trả cho người lao động cũng được tính theo galông* rượu Rum, và tất cả các giao dịch đều được định giá theo lượng rượu Rum. Nhưng dù rượu Rum được xem là nơi cất trữ giá trị tốt hơn ngũ cốc hay thịt, nó vẫn có thể bị sao chép, giả mạo và rất khó khăn trong việc vận chuyển hoặc sử dụng cho các giao dịch lớn.

* Galông là đơn vị đo lường chất lỏng, 01 galông tương ứng với 4,54 lít tại Anh và 3,78 lít tại Mỹ.

Vàng, bạc và các kim loại quý cũng là nơi cất trữ giá trị suốt hàng nghìn năm qua. Giống như rượu Rum, chúng cũng phải đối mặt với đủ loại chi phí như chi phí vận chuyển và chi phí lưu trữ, và đó là lý do tại sao các ngân hàng và tổ chức chính phủ thường cất trữ vàng hay bạc trong kho, đồng thời phát hành những tờ giấy bạc với mệnh giá được đảm bảo bằng kim loại quý. Các kim loại quý có thể duy trì giá trị ổn định dù được cất giữ trong khoảng thời gian gần như là vô hạn. Và các tờ giấy bạc và đồng tiền xu được phát hành với sự đảm

bảo đến từ các kim loại quý, sẽ trở nên dễ dàng vận chuyển và trao đổi hơn, so với vàng hay bạc.

Vàng kỹ thuật số hay tiền kỹ thuật số

Có hai quan điểm khác nhau về Bitcoin. Một số người tin rằng nó nên được xem như vàng kỹ thuật số, một nơi cất trữ giá trị, trong khi nhiều người khác cho rằng nó phải là một loại tiền tệ được sử dụng để trao đổi.

Quan điểm đầu tiên là dựa trên một thực tế là chỉ có 21 triệu bitcoin được tạo ra. Bởi vì chúng hạn chế về số lượng, chúng nên được giao dịch như một mặt hàng giống như vàng, và chủ yếu là một nơi cất trữ giá trị.

Đối với các quốc gia như Zimbabwe, nơi mà đồng nội tệ không được coi là nơi cất trữ giá trị, và việc tích trữ vàng, bạc, đá quý hoặc các loại tiền tệ khác trong nhà sẽ gặp rủi ro bị trộm cắp hoặc hỏa hoạn, nên Bitcoin cung cấp một giải pháp thay thế khả thi khi đóng vai trò như một nơi cất trữ giá trị. Bitcoin cho phép mọi người khởi tạo ví điện tử chỉ trong vài phút, và tích trữ tài sản của mình mà vẫn giữ được giá trị, vẫn được chấp nhận như một phương tiện trao đổi, có thể vận chuyển và được xem là giải pháp an toàn hơn so với các lựa chọn khác.

Bitcoin tồn tại không chịu sự kiểm soát của chính phủ, ngân hàng, và các tổ chức tài chính. Vô số trường hợp trên khắp thế giới nơi mà chế độ độc tài chiếm quyền kiểm soát một quốc gia, thay đổi loại tiền tệ hiện hành, đồng thời tuyên bố tất cả các tờ giấy bạc được lưu thông trước đó là vô giá trị, tái sắp đặt của cải ở nước đó. Tuy nhiên, Bitcoin cho phép người dân ở các nước nơi chính quyền và ngân hàng bất ổn có thể lưu trữ của cải mà không phải chịu sự kiểm soát của chính phủ hay hệ thống tài chính mục nát.

Một quan điểm khác về Bitcoin: Nó không phải nơi cất trữ giá trị mà là một loại tiền tệ để trao đổi. Quan điểm này không coi nó giống như vàng mà như đồng đô la Mỹ, nơi mà số lượng bitcoin không chỉ giới hạn trong con số 21 triệu.

Chúng ta đã chứng kiến sự mất giá trị rất lớn của đồng đô la Zimbabwe, và điều này sẽ mở rộng khả năng cho Bitcoin, nếu bitcoin có số lượng vô hạn nhưng lại tiềm ẩn nguy cơ mất giá. Mặc dù nó có thể được sử dụng như một phương thức trao đổi, nhưng lại không được coi là nơi cất trữ giá trị. Điều này có thể làm gia tăng số lượng giao dịch Bitcoin, nhưng lại càng dễ khiến nó trở nên giống như đồng riel Campuchia, một đồng tiền chỉ được sử dụng cho các giao dịch nhỏ, hoặc không được sử dụng để cất trữ giá trị.

Tổng kết chương 2

Bây giờ, bạn chắc hẳn đã có sự hiểu biết nhất định về cách thức tiền và hệ thống tài chính hoạt động, cùng với lý do tại sao Bitcoin lại có ích như một nơi cất trữ giá trị và phương tiện trao đổi. Trong các chương tiếp theo, chúng ta sẽ tìm hiểu về lịch sử hình thành Bitcoin và chi tiết về cách thức hoạt động của Bitcoin.

Chương 3Lịch sử hình thành Bitcoin

“Tôi nghĩ Internet sẽ là một trong những lực lượng chính làm suy giảm vai trò của chính phủ. Điều duy nhất còn thiếu nhưng sẽ sớm phát triển là một đồng tiền điện tử đáng tin cậy.”

- Milton Friedman, người đoạt giải Nobel Kinh tế

Một trong những công nghệ nền tảng của Bitcoin là Blockchain. Blockchain đầu tiên được tạo ra trong mã máy tính gốc của Bitcoin, và lịch sử hình thành Bitcoin gắn bó chặt chẽ với lịch sử hình thành Blockchain. Cách thức hoạt động của Bitcoin và công nghệ đằng sau nó sẽ được đề cập cụ thể trong chương tiếp theo, vì vậy đừng lo lắng nếu bạn chưa hiểu tường tận về các công nghệ được đề cập ở chương này.

Trong chương này, chúng ta sẽ bàn về lịch sử hình thành Bitcoin cùng với lịch sử của một số công trình và công nghệ nền tảng đã mở đường cho sự ra đời của Bitcoin.

Các giao dịch và hoạt động lưu trữ hồ sơ

Trong chương trước, chúng ta đã tìm hiểu về lịch sử của tiền tệ. Trong chương này, trước hết, chúng ta sẽ tìm hiểu về việc lập hồ sơ giao dịch, một hoạt động được cho là xuất hiện trước khi chữ viết đầu tiên ra đời, bởi vì một số bản viết tay cổ xưa nhất được các nhà khảo cổ học khám phá ra có nội dung liên quan đến giao dịch giá trị.

Một trong những công nghệ nền tảng của Bitcoin là Blockchain. Phần giải thích chi tiết về cách thức hoạt động của Blockchain sẽ được trình bày trong các nội dung sau của cuốn sách, nhưng bây giờ chúng ta sẽ diễn giải thật đơn giản.

Blockchain là một chuỗi các khối được liên kết với nhau bằng mật mã. Mỗi khối chứa một nhóm các giao dịch, và khi một khối xác định được thêm vào Blockchain, các giao dịch trong khối đó được lưu vào Blockchain và không thể bị thu hồi.

Như đã nói, một số bản viết tay đầu tiên có nói về các giao dịch giá trị, được khắc vào đá hoặc các tấm đất sét, và được chính phủ cầm quyền lưu trữ. Hàng ngàn năm trước, người Sumer cổ đại đã ghi chép lại các giao dịch bất động sản, nông sản và những thương vụ trao đổi khác có giá trị trên các khối này.

Các giao dịch này không thể bị thay đổi một khi được lưu lại và mỗi khối bao gồm các giao dịch mới sẽ được thêm vào sau nhóm các khối hiện có. Cứ như vậy, Blockchain đã có lịch sử hàng ngàn năm, với các nguyên tắc về cách thức hoạt động rất giống với những gì mà tài liệu cổ xưa ghi chép lại về các giao dịch.

Mật mã học là một nền tảng khác của Bitcoin, và cũng có tuổi đời hàng ngàn năm. Thật vậy, mật mã cổ đại được sử dụng để bảo vệ các bí mật hoặc các thông điệp chiến lược đối với các chính quyền hoặc lực lượng quân đội.

Một ví dụ nổi tiếng về mật mã cổ đại là Mật mã

Caesar, được đặt theo tên Julius Caesar, người đã mã hóa các văn bản thông tin liên lạc theo phương pháp này. Các đoạn tin nhắn được mã hóa theo mật mã Caesar, trong đó mỗi ký tự được thay thế bằng một ký tự cách nó một số các ký tự cụ thể.

Ví dụ, nếu tất cả các chữ cái đều được di chuyển về phía trước chúng sau 2 chữ cái, A sẽ trở thành C, B sẽ trở thành D và cứ như thế. Sử dụng phương pháp này trên bảng chữ cái tiếng Anh, từ “attack” sẽ trở thành “cvvcem”.

Ở đây, chỉ có những người biết con số cụ thể mà những chữ cái được di chuyển mới có thể giải mã và đọc được đoạn tin nhắn. Ngày nay, loại mật mã này được giải mã dễ dàng, tuy nhiên vào thời đại đó, hầu hết mọi người đều không thể đọc hoặc viết, và bên cạnh

đó cũng có rất nhiều những ngôn ngữ khác nhau trên khắp thế giới có thể được sử dụng để mã hóa trong việc truyền tải thông tin, chứ không nhất thiết phải là ngôn ngữ bản địa. Theo đó, vào thời bấy giờ, phương pháp này vẫn đủ hiệu quả để các đoạn tin nhắn mã hóa không dễ bị kẻ thù giải mã hoặc nghĩ rằng nó đã được viết bằng ngôn ngữ nước ngoài.

Trong khi việc lưu trữ hồ sơ cùng với ngành mật mã học đã được cải tiến rất nhiều kể từ thuở sơ khai, thì các nguyên tắc căn bản làm nền tảng cho Bitcoin vẫn được giữ nguyên. Dữ liệu giao dịch được ghi lại trên các khối là không thể thay đổi được, và dữ liệu đó được mã hóa bằng cách ứng dụng mật mã học, vì vậy chỉ những người có quyền truy cập mới giải mã được.

Phải nói rằng, từ xưa tới nay, có rất nhiều những sáng tạo và sự phát kiến quan trọng trong các lĩnh vực về lưu giữ hồ sơ và mật mã học, tuy nhiên, chúng ta sẽ tạm gác lại để tập trung vào lịch sử của Bitcoin. Trước hết, chúng ta sẽ tìm hiểu về khoảng thời gian những năm 1980, công trình sáng tạo đầu tiên ra đời, mở đường cho sự hình thành Bitcoin.

David Chaum là một trong những người tiên phong trong lĩnh vực thanh toán điện tử, ông được công nhận là người đầu tiên sáng tạo ra tiền kỹ thuật số. Năm 1982, ông đã viết một nghiên cứu có tên là Blind Signatures for Untraceable Payments (tạm dịch: Chữ ký mù cho khoản thanh toán không thể truy nguyên) phác họa tổng quan cách thức các chữ ký mù có thể mã hóa nội dung tin nhắn, trong khi vẫn cho phép xác nhận chữ ký của tin nhắn. Đây là một trong số những công trình được ra đời sớm nhất về chữ ký mã hóa hiện được sử dụng trong Bitcoin và nhiều loại tiền mã hóa khác.

Xử lý vấn đề giao dịch lặp chi là ngăn chặn tình trạng số tiền bị chi tiêu nhiều hơn một lần. Với những tờ đô la Mỹ, chúng chỉ là được làm bằng giấy, vì vậy về lý thuyết, bạn có thể quét và in ra bản sao của mỗi tờ giấy bạc để chi tiêu nhiều lần. Tuy nhiên, trên thực tế có các biện pháp an ninh như họa tiết chìm, chuỗi số duy nhất cho mỗi tờ tiền cùng với hình phạt đối với hoạt động làm giả. Các biện pháp an ninh và pháp lý này là cách chính phủ Mỹ ngăn chặn tái diễn giao

dịch lặp chi đồng đô la Mỹ, khi mỗi tờ tiền đều không thể sao chép được.

Việc ngăn ngừa tình trạng giao dịch lặp chi trong lĩnh vực tiền điện tử lại phức tạp hơn nhiều. Bạn có thể hình dung thế này, nếu những khoản thanh toán cho hàng hóa hay dịch vụ đều trong môi trường điện tử như dưới dạng email, vậy làm thế nào bạn có thể ngăn chặn việc một email có nội dung thanh toán tương tự được gửi đến nhiều người? Các chính phủ, ngân hàng và tổ chức tài chính có các lớp thủ tục xác minh để đảm bảo không có xuất hiện bản sao các giao dịch điện tử, ngay cả khi những hệ thống này có khả năng gặp trục trặc.

Trong lĩnh vực tiền điện tử, với sự cộng tác của Amos Fiat và Moni Naor, David Chaum đã đề xuất nhiều giải pháp cho vấn đề giao dịch lặp chi.

Những bản đề xuất của họ đưa ra một lý thuyết cho rằng: tiền điện tử có thể mang đặc tính không bị truy nguyên, nhưng vẫn có thể bị phát hiện nếu đã được chi tiêu từ trước đó.

Năm 1990, David Chaum thành lập công ty DigiCash cùng với những người tiên phong trong lĩnh vực này. Năm 1994, DigiCash đã gửi đi khoản thanh toán bằng tiền điện tử đầu tiên.

Cũng năm 1994, một thông cáo báo chí được DigiCash phát hành, với nội dung mở đầu như sau:

“Khoản thanh toán bằng tiền điện tử đầu tiên qua mạng máy tính trên thế giới. (Ngày phát hành: 27, tháng 5 năm 1994)

Tiền điện tử có sự riêng tư của tiền giấy, trong khi nó vẫn đạt được yêu cầu về bảo mật cao đối với các môi trường mạng lưới điện tử thông qua những đổi mới trong mật mã khóa công khai.”

Thông cáo báo chí này của DigiCash được phát hành vào thời điểm 14 năm trước khi Bitcoin ra đời. Và một thông cáo báo chí với nội dung tương tự có thể sử dụng cho Bitcoin khi nó được phát hành.

DigiCash có lẽ đã phát triển quá sớm trong lĩnh vực thương mại điện tử so với thời đại, khi mà vào năm 1994, vẫn chưa có nhiều người dùng Internet.

Hệ quả là, năm 1998, DigiCash tuyên bố phá sản, và tài sản còn lại bị bán cho eCash Technologies.

Trong quá trình nghiên cứu, DigiCash đã sử dụng chữ ký cá nhân/công khai được mã hóa để ẩn giấu và xác minh nội dung tin nhắn, đồng thời là tiền điện tử đầu tiên có đặc tính không thể truy nguyên và tránh được tình trạng giao dịch lặp chi. Và tất cả những tính năng này đã đặt nền móng cho Bitcoin, cũng như các đồng tiền mã hóa xuất hiện sau Bitcoin.

Khi Internet bắt đầu trở nên phổ biến, thư rác trở thành một vấn nạn. Adam Back đã đề xuất một phương pháp chống nạn gửi thư rác tràn lan và các cuộc tấn công từ chối dịch vụ.

Vào năm 1997, Adam Back đã tạo ra “hashcash” - một thuật toán đơn giản sử dụng Bằng chứng Xử lý để ngăn chặn thư rác. Thuật toán Bằng chứng Xử lý trong hashcash đòi hỏi hệ thống máy tính gửi thư điện tử phải giải đáp một mảnh ghép toán học và đưa ra câu trả lời trong tiêu đề thư.

Một câu trả lời hợp lệ trong tiêu đề thư chính là bằng chứng cho thấy sự đóng góp nguồn lực và công suất tính toán đã được sử dụng để gửi thư điện tử đó. Trong trường hợp không có Bằng chứng Xử lý hợp lệ trong tiêu đề, thư điện tử đó có thể bị lọc ra là thư rác.

Phương pháp này giúp cho việc gửi thư điện tử trở nên ít tốn kém hơn đối với hầu hết mọi người, nhưng lại tiêu tốn thời gian và tốn nguồn lực nhiều hơn nếu muốn gửi đi một lượng lớn thư rác. Khi Bitcoin được tạo ra, nó được tích hợp một thuật toán cao cấp hơn nhưng lại tương tự như thuật toán Bằng chứng Xử lý.

Nick Szabo là người tiên phong khác trong thời kì đầu của tiền kỹ thuật số. Năm 1998, ông đưa ra đề xuất cho một loại tiền kỹ thuật

số phi tập trung có tên “bit gold”. Đồng tiền này tích hợp nhiều đặc điểm từ DigiCash cùng với thuật toán Bằng chứng Xử lý, mà tại đó các nguồn lực tính toán đều dành để giải đáp các mảnh ghép mật mã toán học. Giải các mảnh ghép toán học này sẽ giống như việc tìm kiếm sự kết hợp với khóa; không dễ để tìm ra, nhưng một khi thu được câu trả lời, thì việc kiểm nhận nó có chính xác hay không rất dễ dàng.

Bất cứ ai trên mạng lưới đều có thể dễ dàng xác nhận câu trả lời là đúng, tuy nhiên, đa số những thành viên trong mạng lưới sẽ phải đồng ý rằng nó hợp lệ trước khi nó được chấp nhận. Một yếu tố bổ sung khác mà Nick Szabo thêm vào thuật toán Bằng chứng Xử lý là câu trả lời cho một mảnh ghép toán học sẽ trở thành một phần của mảnh ghép toán học tiếp theo. Điều này kết nối chúng lại với nhau như một chuỗi, từ đó tạo ra một trình tự các mảnh ghép, đáp án và giao dịch liên kết với chúng rõ ràng theo thời gian.

Mặc dù đề xuất Bit Gold của Nick Szabo chỉ tồn tại trên lý thuyết, nhưng nó được xem như đang đặt những viên gạch nền tảng cho việc xây dựng Bitcoin sau này.

Cũng năm 1998, một chuyên đề của Wei Dai đã được xuất bản với nhan đề b-money, an Anony- mous, Distributed Electronic Cash System (tạm dịch: b-money, một hệ thống tiền điện tử phân tán, ẩn danh). Bài viết này sau đó đã được nhắc đến trong chuyên đề giới thiệu Bitcoin.

Trong bài báo của Wei Dai về b-money, ông đề xuất một hệ thống tiền điện tử có:

• Bằng chứng Xử lý thông qua nguồn lực tính toán được đóng góp cho hệ thống

• Những phần thưởng cho việc hoàn thành Bằng chứng Xử lý hợp lệ

• Tất cả thành viên của hệ thống đều có thể xác minh và cập nhật sổ cái chung

• Các giao dịch trên sổ cái của nhóm được xác minh qua mã băm

• Chữ ký kỹ thuật số sử dụng mật mã học để ký và xác minh các giao dịch trên sổ cái chung

Hệ thống tiền điện tử b-money được đề xuất bởi Wei Dai cũng chỉ tồn tại trên lý thuyết, tuy nhiên, Bitcoin sau đó đã tích hợp nhiều tính năng được đề xuất bởi b-money trong quá trình hình thành.

Satoshi Nakamoto được coi là người sáng tạo ra Bitcoin. Và người ta thường chấp nhận một điều rằng, Satoshi Nakamoto là chỉ một bút danh, và người này chưa bao giờ tiết lộ công khai thân phận của mình.

Mười năm sau thời điểm đề xuất về b-money của Wei Dai ra đời, Satoshi Nakamoto đã xuất bản một bài báo trên Internet vào năm 2008 có tiêu đề là Bitcoin: A Peer-to-Peer Electronic Cash System (tạm dịch: Bitcoin: Hệ thống tiền ảo ngang cấp). Bài báo này đã tích hợp nhiều yếu tố của các nghiên cứu trước đây về tiền kỹ thuật số, các loại tiền tệ theo mô hình phi tập trung, các khoản thanh toán không thể theo dõi, Bằng chứng Xử lý và mật mã, thành một giải pháp khả thi.

Một năm sau đó, tức là vào năm 2009, Bitcoin được tạo ra và trở thành loại tiền kỹ thuật số phi tập trung đầu tiên thực tồn chứ không chỉ trên tài liệu khoa học. Blockchain đầu tiên cũng được tạo ra trong mã Bitcoin, được viết trong mã bằng hai từ riêng biệt chuỗi (chain) và khối (block).

Satoshi Nakamoto khai thác khối đầu tiên trên mạng lưới Bitcoin, được biết đến với tên Khối Nguyên thủy. Khối Nguyên thủy do Satoshi Nakamoto khai thác có chứa thông điệp:

“Tờ Times, ngày 03/01/2009, Đại Pháp Quan đứng bên bờ vực phải viện trợ ngân hàng lần thứ hai”.

Thông điệp này được đưa vào khối đầu tiên như là một bằng chứng cho thấy khối đầu tiên này của Blockchain Bitcoin được khai thác

vào ngày mùng ba tháng Một hoặc sau đó. Đây còn là tuyên bố về những thất bại của tiền tệ và thị trường tài chính hiện hành.

Tiêu đề này được lấy từ một bài báo xuất bản ở Anh, và khiến người ta nghĩ rằng Satoshi Nakamoto sinh sống ở Vương quốc Anh tại thời điểm đó.

Năm 2010, đã có nhiều vấn đề lớn được tìm thấy trong mạng lưới Bitcoin cho phép các giao dịch có thể bị thay đổi. Điều này đã dẫn đến một lượng lớn bitcoin bị tạo ra sai trái so với quy tắc của hệ thống. Lỗi này nhanh chóng được phát hiện, các giao dịch giả mạo Bitcoin đã bị xóa bỏ, và kể từ đó không xảy ra hiện tượng như thế nữa.

Trong năm 2011, trang web Silk Road ra mắt, nó cho phép mọi người buôn bán ma túy trực tuyến trả bằng Bitcoin. Điều này đã dẫn đến sự gia tăng nhu cầu về Bitcoin, đồng thời Bitcoin cũng đã trở nên nổi tiếng bởi nó được sử dụng chủ yếu trong hoạt động buôn bán ma túy và các hoạt động tội phạm.

Trong một vài năm sau đó, Bitcoin ngày càng phổ biến. Giá của Bitcoin đã tăng từ khoảng 1 đô la Mỹ năm 2011 lên khoảng 1.000 đô la vào năm 2013. Thêm vào đó, thị trường buôn bán ma túy trên Silk Road ngày càng trở nên nổi tiếng trong những năm đó, khi ngày càng có nhiều sự liên kết giữa Bitcoin với ma túy và tội phạm hơn.

Vào năm 2013, mọi thứ trở nên tiêu cực đối với Bitcoin: FBI đóng cửa vĩnh viễn trang web Silk Road, đồng thời tịch thu tất cả tài sản trên đó, và người sáng lập Silk Road bị kết án tù chung thân. Đáng chú ý là, người sáng lập đã bị bắt khi ông ta cố gắng trả lương bằng bitcoin cho một cảnh sát nằm vùng giả làm một lính đánh thuê trên trang web Silk Road để nhận sát hại một ai đó. Đây là một tin tức gây chú ý lớn vào thời điểm đó, và nó không giúp cải thiện danh tiếng của Bitcoin trong tâm trí của công chúng.

Thậm chí, mọi chuyện trở nên tồi tệ hơn với Bitcoin khi sàn giao dịch Bitcoin lớn nhất Mt. Gox cho ngừng rút tiền bằng đô la Mỹ, và tuyên bố phá sản vào đầu năm 2014. Tại thời điểm đó, sàn Mt. Gox

nắm giữ khoảng 70% tổng số các giao dịch liên quan tới Bitcoin, và khi sàn tuyên bố phá sản, nhiều người đã mất hết số bitcoin của mình.

Những sự kiện này khiến Bitcoin giảm giá từ khoảng 1.000 đô la xuống còn khoảng 200 đô la trong năm kế tiếp. Sau đó, các đồng tiền mã hóa mới được tạo ra bằng mã nguồn Bitcoin, và nhiều người tuyên bố rằng Bitcoin đã chấm hết.

Tuy nhiên, Bitcoin không sụp đổ, và nhờ việc trang Silk Road bị đóng cửa, Bitcoin dần bớt liên quan tới ma túy, sát nhân và tội phạm. Nhóm xây dựng Bitcoin cốt lõi tiếp tục thực hiện các cải tiến về mã nguồn Bitcoin. Và mọi người bắt đầu chú ý dẫn đến công nghệ nền tảng đằng sau Bitcoin và hiểu hơn về tiềm năng của nó.

Những người nhìn vào công nghệ nền tảng đằng sau Bitcoin đã thấy được sự kỳ diệu về cách thức nó hoạt động ra sao, nhưng vẫn rất khó để kêu gọi nguồn tài trợ nghiêm túc cho các dự án liên quan đến Bitcoin. Nhiều công ty và chính phủ vẫn coi Bitcoin là tiền Internet giả mạo, cụ thể hơn, họ chỉ coi nó là một trào lưu nhất thời hay một vụ lừa đảo. Các công ty lớn và các tổ chức tài chính không muốn dính líu tới Bitcoin, bởi vì họ vẫn thấy nó có liên quan quá chặt chẽ tới sự phá sản của Mt. Gox và lực lượng tội phạm trên Silk Road.

Blockchain, một trong những công nghệ chính của Bitcoin, lại được nhiều người tin là một công nghệ mang tính cách mạng như Internet. Khi công nghệ Blockchain và những nền tảng đằng sau Bitcoin trở nên ít liên quan đến chính Bitcoin, các công ty háo hức và sẵn sàng chi tiền đầu tư nghiên cứu và phát triển các công nghệ về Blockchain.

Bắt đầu xuất hiện sự tách biệt rõ ràng giữa Bitcoin và các công nghệ bên trong mã nguồn Bitcoin. Mặc dù các công ty không dành sự quan tâm đặc biệt cho Bitcoin, nhưng họ lại rất chú ý tới tiềm năng áp dụng Blockchain và các công nghệ bên trong Bitcoin.

Vào năm 2015, mạng lưới Ethereum đã ra đời, làm gia tăng sự chú ý tới Blockchain và tiền mã hóa. Ethereum đã tạo ra những triển vọng mới cho công nghệ Blockchain với các ứng dụng phi tập trung và các hợp đồng thông minh khả dụng trên Blockchain. Kể từ khi Ethereum ra mắt, đã có hàng ngàn công ty bắt tay vào việc ứng dụng công nghệ Blockchain cho một loạt các ngành công nghiệp khác nhau. Điều này đã dẫn đến sự phổ biến của Bitcoin và các đồng tiền mã hóa khác.

Mặc dù Ethereum được xem là có nhiều ứng dụng tiềm năng hơn so với công nghệ Bitcoin hiện tại, nhưng Ethereum không được thiết kế để thay thế cho Bitcoin trong các hoạt động liên quan đến các giao dịch tài chính hoặc thanh toán. Sự gia tăng số lượng các đồng tiền mã hóa và mối quan tâm tới Blockchain đã nâng cao tiếng tăm của Bitcoin với vai trò một hình thức thanh toán đạt mức giá kỷ lục trên 3.000 đô la Mỹ vào năm 2017.

Tổng kết chương 3

Dù hiện nay, Bitcoin ít liên quan đến các hoạt động tội phạm và ma túy, nhưng nó vẫn chưa được phần đông mọi người chấp nhận hoặc sử dụng chính thức. Mặc dù trên thực tế, Coinbase, Circle và các công ty tương tự cho phép thực hiện các hoạt động mua bán và giao dịch bitcoin dễ dàng như dịch vụ ngân hàng trực tuyến, tuy nhiên, hầu hết mọi người vẫn không thấy việc này là cần thiết hoặc không hiểu cách sử dụng Bitcoin. Dường như, công nghệ mới cần nhiều thời gian hơn mới được chấp thuận và áp dụng rộng rãi, mà Bitcoin vẫn còn trong thời kì đầu của nó.

Mặc dù không có gì chắc chắn về tương lai của Bitcoin, nhưng nó đã trở nên mạnh mẽ hơn mỗi khi phải đối mặt với trở ngại và ngay cả khi bị tuyên bố đã chấm hết. Xu hướng hiện tại có lẽ vẫn coi Bitcoin như một giải pháp thanh toán khả thi bên cạnh thẻ tín dụng, Paypal và các tùy chọn thanh toán hiện có khác.

Đến lúc này, bạn đã có hiểu biết nhất định về khái niệm Bitcoin và lịch sử phát triển của nó. Trong chương kế tiếp, chúng ta sẽ tìm hiểu xem Bitcoin và công nghệ nền tảng của nó hoạt động như thế nào.

Chương 4Cách thức hoạt động của Bitcoin

“Lần đầu tiên nghe nói về Bitcoin, tôi đã nghĩ nó thật bất khả thi. Làm sao bạn có thể sở hữu đồng tiền kỹ thuật số thuần túy này?

Chẳng lẽ tôi không thể sao chép ổ cứng của bạn để chiếm lấy bitcoin của bạn ư? Tôi đã không hiểu bằng cách nào đồng tiền này vượt qua được điều đó, nhưng giờ nhìn lại, tôi thấy nó thật tuyệt vời.”

– Jeff Garzik, nhà phát triển nòng cốt của Bitcoin

Lưu ý: Chương này là bản hướng dẫn tổng quan, không nặng tính kỹ thuật về cách thức hoạt động của Bitcoin.

Chỉ dẫn căn bản về cách thức hoạt động của Bitcoin

Như đã đề cập trong các nội dung trước, tiền hiện đại chỉ là những con số điện tử trên máy tính và các ngân hàng, chính phủ và tổ chức tài chính có chức năng cất trữ những hồ sơ chi tiết về nơi mà mỗi con số điện tử hoặc mỗi đơn vị tiền tệ được lưu giữ.

Bitcoin không có chính quyền hay ngân hàng trung ương theo dõi hồ sơ giao dịch, và cũng không thể tự mình phát hành tiền mới. Bởi Bitcoin là một loại tiền mã hóa và không chịu kiểm soát của tổ chức nào trong việc quản lý hồ sơ, nên nhiều người cho rằng nguy cơ nó bị hacker tấn công để tạo bitcoin giả hoặc giao dịch giả cao hơn so với các loại tiền truyền thống. Tuy nhiên, thực tế hoàn toàn ngược lại, Bitcoin ít gặp rủi ro bị tấn công, giả mạo và sao chép giao dịch hơn hẳn so với đồng tiền hiện đại.

Không tồn tại chính phủ hay ngân hàng trung ương nào là đơn vị phát hành bitcoin hoặc theo dõi hồ sơ giao dịch bitcoin. Cấu trúc phi tập trung của Bitcoin đồng nghĩa với tất cả mọi người trên mạng

lưới đều tham gia xác nhận rằng những hồ sơ và giao dịch là hoàn toàn chính xác. Bất cứ khi nào một giao dịch diễn ra, tất cả mọi người trên mạng lưới đều có một bản hồ sơ về giao dịch đó, và đa số mọi người phải đồng thuận là nó hợp lệ.

Trong ví dụ trước đây, một tờ giấy bạc với dòng chữ "Tôi nợ bạn 100 đô la" có thể được bạn của bạn chấp nhận – người này tin rằng họ có thể nhận lại giá trị đó từ bạn trong tương lai. Tuy nhiên, bạn của bạn không thể ra ngoài và trao nó cho một chủ cửa hàng hay bất kì ai khác, bởi vì họ không tin họ có thể sử dụng tờ giấy bạc đó ở nơi khác.

Để hiểu về cách thức hoạt động của Bitcoin và tất cả các đồng tiền kỹ thuật số, hãy xem xét ví dụ sau đây. Tưởng tượng bạn và 10 người bạn khác thường xuyên mua bán các mặt hàng hoặc dịch vụ của nhau. Theo đó, thay vì liên tục đổi tiền qua lại cho nhau, bạn có một hệ thống mà trong đó mỗi người sở hữu 500 đô la và số tiền này có thể được chuyển giao thông qua email như một khoản thanh toán. Khi một người bạn nhận được email với số tiền đó, họ có thể gửi email đó cho một người bạn khác để thanh toán.

Cụ thể hơn nữa, giả sử bạn của bạn là John, John bán cho bạn một chiếc tivi với giá 100 đô la, nhưng thay vì trả John 100 đô la tiền mặt hoặc tờ ghi nợ, bạn gửi cho John một email có dòng chữ là "Email này có giá 100 đô la".

Trong trường hợp này, với việc ban đầu cả hai bạn đều có 500 đô la, sau khi giao dịch diễn ra, bạn sẽ có số dư là 400 đô la còn của John là 600 đô la.

John sau đó muốn mua một chiếc bàn từ Sally với giá 100 đô la, John gửi đi email mà anh ấy đã nhận từ bạn như một khoản thanh toán.

Trong những trường hợp này, sẽ rất dễ dàng để viết một email với cùng nội dung và gửi cho bất cứ ai để thanh toán. Vì sẽ không có gì ngăn cản John gửi email thanh toán 100 đô đó cho cả 10 người bạn

của anh ấy, để nhận về 1.000 đô giá trị hàng hóa trong khi những người kia, về bản chất, không thu được số tiền này.

Đây được gọi là giao dịch lặp chi, một vấn nạn mà đồng tiền mã hóa đã phải vật lộn giải quyết. Tuy nhiên, Bitcoin đã giải quyết thành công vấn đề này.

• Khi một email được gửi đến mạng lưới bạn bè này, tất cả mọi người đều nhận được bản sao email đó.

• Khi bạn gửi 100 đô la cho John, tất cả những người còn lại trong mạng lưới đều sẽ biết về sự tồn tại của giao dịch này.

• Khi John gửi số tiền này cho Sally, mọi người cũng nhận được bản sao email gửi đi, nên họ đều biết 100 đô la đã được gửi từ bạn tới John, sau đó lại tiếp tục được gửi từ John tới cho Sally.

• Nếu bạn cố gắng gửi 100 đô la đến 10 người bạn cùng một lúc, họ đều sẽ nhận được bản sao những email này, đều biết rằng chúng không hợp lệ, và kết luận rằng bạn đang cố gắng chi tiêu khoản tiền mà bạn không hề sở hữu.

• Đa số thành viên trong mạng lưới phải đồng ý rằng giao dịch đó là hợp lệ. Mỗi khi giao dịch diễn ra, nó sẽ được gửi đến mọi thành viên trong mạng lưới để quyết định xem giao dịch đó có hợp lệ hay không.

• Một giao dịch hợp lệ sau đó sẽ được ghi chép lại trên mạng lưới, mỗi người sẽ nhận được bản sao cập nhật gồm các giao dịch hợp lệ đó, vì vậy họ đều biết thông tin về tất cả các giao dịch đã xảy ra.

Cách thức bitcoin hoạt động như thế nào sẽ được đề cập chi tiết hơn trong phần sau cuốn sách này, tuy nhiên, ví dụ này đã cung cấp cho bạn một hình dung căn bản về cách mạng lưới Bitcoin ngăn chặn tình trạng giả mạo bitcoin và sao chép các giao dịch. Tất cả mọi người trên mạng lưới đều tham gia xác minh tính hợp lệ của các giao dịch, duy trì các hồ sơ lưu trữ, và luôn nhận thức được những gì đang xảy ra trên mạng lưới.

Blockchain là gì?

Có rất nhiều giao dịch xuất hiện trên mạng lưới cùng một lúc. Khi giao dịch Bitcoin được ghi chép, nó được tập hợp lại cùng với các giao dịch khác thành một khối các giao dịch.

Các giao dịch được lưu trữ trên mạng lưới theo nhóm khi một khối mới được thêm vào mạng lưới. Một khối mới được thêm vào ngay trên khối gần nhất, khối gần nhất này lại liên kết với khối liền trước đó nữa, như thế tất cả các khối sẽ liên kết với nhau thành một chuỗi.

Ví dụ:

Khối 100 liên kết với khối 99

Khối 99 liên kết với khối 98

Khối 98 liên kết với khối 97

Điều này cứ thế tiếp tục cho đến khối đầu tiên của Blockchain, khối 0, hay còn gọi là Khối Nguyên thủy.

Một khối mới các giao dịch sẽ được thêm vào Blockchain Bitcoin khoảng 10 phút một lần. Tất cả các giao dịch xuất hiện đều được lưu lại trong Blockchain và bất khả sửa đổi. Vì vậy, các giao dịch trên Blockchain Bitcoin đều có thể được truy dấu từ khối mới nhất cho tới khối đầu tiên trong Blockchain.

Sửa đổi giao dịch và khối

Một khi một khối các giao dịch được thêm vào Blockchain Bitcoin, nó không thể bị thay đổi hoặc thu hồi. Hơn nữa, các giao dịch trong mỗi khối được nhóm lại với nhau và được mã hóa, mỗi nhóm giao dịch có dữ liệu mã hóa độc nhất vô nhị.

Khi một khối được liên kết với khối trước đó, nó được liên kết bằng cách sử dụng dữ liệu được mã hóa riêng biệt. Nếu một người cố gian lận bằng cách thay đổi thông tin của các giao dịch trong một

khối, họ phải thay đổi dữ liệu đã được mã hóa riêng biệt. Hành động này sẽ phá vỡ chuỗi các khối vì chúng sẽ không còn cho thấy dữ liệu khối chính xác nữa.

Nếu xem lại lịch sử của Bitcoin, chúng ta sẽ thấy phương pháp Bit Gold của Nick Szabo đã cho thấy đáp án cho một mảnh ghép toán học trở thành một phần trong mảnh ghép toán học tiếp theo. Nếu ai đó cố gắng thay đổi giao dịch trong một khối, họ sẽ làm thay đổi câu trả lời cho mảnh ghép toán học đó, và mảnh ghép này sẽ không còn phù hợp với câu hỏi của mảnh ghép tiếp theo nữa. Tình trạng này tiếp tục làm thay đổi câu trả lời cho mảnh ghép toán học sau đó nữa, và sự thay đổi cứ như thế sẽ tiếp diễn đến đầu chuỗi.

Vì vậy, để thực hiện hành vi gian lận trên một khối giao dịch trước đó, mỗi khối tiếp sau khối bị chỉnh sửa cũng phải thay đổi theo, và điều này hoàn toàn bất khả thi về mặt tính toán sau 6 khối trên Blockchain Bitcoin.

Hành vi cố gắng thay đổi các giao dịch trong khối 100 sẽ trở nên bất khả thi sau khi có khối 106. Một khối mới được thêm vào Blockchain Bitcoin cứ 10 phút một lần, do đó các giao dịch trong một khối có thể được thay đổi trong vòng một giờ nếu phần lớn các máy tính trên mạng lưới đều chấp thuận sự thay đổi này. Sau một giờ, việc thay đổi các giao dịch trên Blockchain Bitcoin trở nên bất khả thi về mặt tính toán.

Các công ty có thể xem các khối như những xác nhận; nếu một giao dịch xảy ra trong khối 100, sau đó các công ty có thể yêu cầu 6 xác nhận trước khi chấp nhận giao dịch là hợp lệ. Một khi 6 khối mới được thêm vào sau khối 100, tương đương với việc có 6 xác nhận rằng giao dịch đó là hợp lệ, nó sẽ không thể bị thay đổi hoặc thu hồi.

Đồng thuận phân tán

Phần lớn các máy tính trên mạng lưới Bitcoin cần chấp nhận các giao dịch và các khối là hợp lệ, quá trình này được gọi là đồng thuận phân tán.

Việc yêu cầu tất cả mọi người trên mạng lưới Bitcoin đồng thuận gần như là không thể, nhưng chỉ cần trên 50% số thành viên trong mạng lưới thì hoàn toàn khả thi. Trên 50% thành viên của mạng lưới đồng ý được coi như bằng chứng phù hợp để xác minh giao dịch hợp lệ.

Đây là một sự khác biệt quan trọng giữa hệ thống tập trung và hệ thống phi tập trung. Với một hệ thống tập trung, quyền quyết định tính hợp lệ của giao dịch được thực hiện bởi một thực thể như ngân hàng hay một cá nhân trong một phòng ban. Lịch sử đã cho thấy vô số các ví dụ điển hình về việc hệ thống tập trung có xu hướng gian lận hoặc nhầm lẫn trong việc nhập thông tin giao dịch hay bị thao túng. Nhưng trong hệ thống phi tập trung, các quyết định này được thực hiện bởi phần lớn các thành viên của mạng lưới, thông tin trong mạng lưới minh bạch với tất cả mọi người và họ đều có thể quan sát tất cả các giao dịch xuất hiện trên mạng lưới Bitcoin.

Chúng ta cũng biết đến nguy cơ xảy ra các cuộc tấn công quá bán, khi một kẻ tấn công có thể kiểm soát trên 50% mạng lưới Bitcoin. Điều này sẽ cho phép kẻ đó quyết định giao dịch nào là hợp lệ và nắm quyền kiểm soát sự đồng thuận của toàn bộ mạng lưới. Tuy nhiên, nguy cơ này rất thấp, bởi cần tới chi phí khổng lồ và công suất tính toán khủng khiếp mới đạt được.

Khai thác Bitcoin

Khai thác là từ mà có lẽ bạn đã nghe nói nhiều trong các tài liệu tham khảo về Bitcoin. Khi các giao dịch được truyền gửi trên mạng lưới Bitcoin, chúng vẫn đang trong trạng thái chờ xử lý cho đến khi được thêm vào một khối trên Blockchain Bitcoin. Các máy tính trên mạng lưới Bitcoin lựa chọn các giao dịch đang chờ xử lý, và nhóm chúng lại thành một khối để thêm vào Blockchain Bitcoin.

Khi một máy tính thêm được một khối hợp lệ vào Blockchain Bitcoin, họ nhận được một khoản thanh toán bitcoin như là phần thưởng cho việc thêm khối đó vào Blockchain. Đây được gọi là “phần thưởng khối” còn quá trình này được biết đến như quá trình “khai thác” vì nó tương tự như việc khai thác những phần thưởng nhỏ ra

khỏi khối lớn. Các máy tính tham gia vào quá trình này được gọi là "thợ đào".

Để thêm được một khối các giao dịch hợp lệ vào Blockchain, các thợ đào trước tiên phải xử lý một mảnh ghép toán học, mà mảnh ghép này chỉ có thể được giải đáp thông qua đoán số ngẫu nhiên. Nếu thợ đào sở hữu công suất tính toán càng lớn, họ càng có khả năng đoán được con số ngẫu nhiên nhanh hơn, đồng thời thêm được một khối hợp lệ vào Blockchain để nhận về những phần thưởng.

Bằng chứng Xử lý

Phần thưởng được trả cho thợ đào đã thêm thành công một khối hợp lệ vào Blockchain là một khoản bù đắp vì những đóng góp về nguồn lực, điện năng và công suất tính toán vào mạng lưới. Công suất tính toán và các nguồn lực được đóng góp cho phép mạng lưới Bitcoin hoạt động hiệu quả và an toàn.

Như đã đề cập trước đó, thợ đào phải giải đáp một mảnh ghép toán học để thêm được một khối hợp lệ vào Blockchain. Đây được gọi là "Bằng chứng Xử lý" bởi nó đòi hỏi một số lượng công việc nhất định dưới dạng công suất tính toán và các nguồn lực để giải quyết. Thợ đào tìm ra đáp án đầu tiên, chứng tỏ họ đã hoàn thành công việc để thêm được một khối vào Blockchain.

Mảnh ghép toán học này tương tự như khóa mật mã, và cần rất nhiều thời gian mới đoán ra mật mã cho khóa; tuy nhiên, một khi tìm ra đáp án, việc xác định nó chính xác hay không rất dễ dàng.

Các thợ đào làm việc để đoán ra con số cho khóa mật mã này, và người tìm thấy câu trả lời đầu tiên có thể công bố cho tất cả mọi người trên mạng lưới. Khi ấy, mọi thợ đào khác đều có thể xác nhận mật mã đó có hợp lệ không, và điều này đóng vai trò như bằng chứng xác minh rằng thợ đào kia đã giải quyết thành công mảnh ghép toán học này. Người thợ đào đó sẽ nhận được phần thưởng cho công việc đã hoàn thành, và tất cả các thợ đào tập trung công

suất tính toán vào việc giải quyết mảnh ghép toán học tiếp theo để lại thêm được khối mới vào Blockchain Bitcoin.

Quá trình đóng góp một lượng lớn công suất tính toán để tìm con số ngẫu nhiên có vẻ không cần thiết và phí phạm. Đây chính là khởi nguồn cho sự chỉ trích lớn về thuật toán Bằng chứng Xử lý trong Bitcoin. Bởi vì một lượng lớn điện năng và công suất tính toán được sử dụng cho quá trình rất lãng phí và không phải là yêu cầu bắt buộc để thêm được các giao dịch mới vào Blockchain Bitcoin.

Bằng chứng Xử lý chủ yếu cố gắng xác minh một điều rằng: Các nguồn lực đã được đóng góp vào mạng lưới, cho thấy các thợ đào đang giúp mạng lưới Bitcoin hoạt động và bảo vệ an ninh cho nó.

Bằng chứng Xử lý là thuật toán được sử dụng trong mạng lưới Bitcoin, còn nhiều thuật toán khác được ứng dụng trong các loại tiền mã hóa khác. Sự lãng phí của thuật toán Bằng chứng Xử lý cùng với các thuật toán thay thế mà nhiều đồng tiền mã hóa khác đang sử dụng sẽ được đề cập chi tiết hơn trong những nội dung sau của cuốn sách.

Tổng kết chương 4

Bây giờ bạn chắc hẳn đã hiểu rõ hơn về những công nghệ nền tảng đằng sau Bitcoin cũng như các nguyên tắc cơ bản về cách thức hoạt động của nó. Trong các chương kế tiếp, chúng ta sẽ cùng xem xét những lợi ích và bất lợi trong việc sử dụng Bitcoin.

Chương 5Lợi ích của Bitcoin

“Về bản chất, bitcoin là một đồng tiền thông minh, được tạo ra bởi các kỹ sư có tư tưởng tiến bộ. Nó giúp loại bỏ sự cần thiết của các ngân hàng, những khoản phí tín dụng, phí quy đổi ngoại tệ, phí chuyển tiền và sự cần thiết của luật sư trong quá trình chuyển nhượng... tất cả đều là những điều tốt đẹp.”

– Peter Diamandis

Trong các chương đầu, chúng tôi đã đề cập đến các nguyên tắc cơ bản của Bitcoin, cách thức hoạt động của Bitcoin và các thị trường tài chính, cũng như lịch sử hình thành Bitcoin. Trong chương này, chúng ta sẽ tìm hiểu một số lợi ích của Bitcoin so với các phương thức thanh toán hiện tại.

Loại bỏ các tổ chức trung gian

Hầu hết các giao dịch hiện đại đòi hỏi phải có một tổ chức trung gian cung cấp sự tin tưởng và đảm bảo. Trong khi đó, Bitcoin cho phép mọi người có khả năng giao dịch trực tiếp với nhau mà không cần đến các tổ chức trung gian.

Ở những nơi như Mỹ hoặc châu Âu, nơi có các quy định đối với tổ chức tài chính và hệ thống pháp luật ổn định, thì đặc tính này có vẻ không phải một yếu tố quan trọng. Tuy nhiên, phần lớn dân cư trên thế giới sống ở các quốc gia, nơi các tổ chức trung gian không hề đáng tin.

Hàng tỷ người trên thế giới đang sống ở những quốc gia, nơi chính phủ và ngân hàng mục nát, tỉ lệ tội phạm cao, các quy định đối với công ty không có hoặc rất ít, hoạt động lưu trữ hồ sơ thường được thực hiện thủ công và các danh mục pháp lý hạn chế.

Bitcoin đặc biệt hữu ích ở những quốc gia mà ở đó người dân thiếu tin tưởng đối với chính phủ, ngân hàng và các tổ chức trung gian.

Hoạt động giao dịch trực tiếp với người dân ở những quốc gia này cũng có thể gặp rủi ro, vì tỷ lệ tội phạm cao và không có danh mục pháp lý cụ thể. Nếu bạn giao dịch trực tiếp với ai đó bằng đồng nội tệ hoặc vàng, họ có thể trộm hoặc không tôn trọng thỏa thuận.

Việc cất trữ và giao dịch bằng bitcoin có thể là một lựa chọn an toàn hơn so với việc giữ tiền trong tài khoản ngân hàng hoặc giao dịch bằng đồng nội tệ tại các quốc gia này. Bitcoin cung cấp sự tin tưởng và bảo mật đồng thời giảm được nhiều rủi ro liên quan đến các giao dịch không cần sự xuất hiện của tổ chức trung gian.

Sự phi tập trung

Như đã đề cập ở trên, hầu hết các giao dịch tài chính hiện nay đều yêu cầu một tổ chức trung gian tham gia giao dịch. Ngay cả một khoản thanh toán trên thẻ tín dụng trong cửa hàng cũng cần có sự xuất hiện của công ty thẻ tín dụng và ngân hàng, vì họ là những tổ chức trung gian đứng giữa người mua và người bán. Các tổ chức trung gian này sở hữu những hệ thống theo mô hình tập trung để ghi lại tất cả các giao dịch và xử lý chúng.

Nếu bạn chuyển tiền từ tài khoản ngân hàng này sang tài khoản thuộc ngân hàng khác, thì khi ấy, mỗi ngân hàng đều có các hệ thống kiểm soát theo mô hình tập trung, và các sổ cái tập trung để ghi chép lại giao dịch của bạn. Bạn có thể gặp phải tình trạng quen thuộc khi gửi giao dịch, tiền ra khỏi tài khoản ngân hàng của bạn, nhưng vài ngày sau mới xuất hiện trong tài khoản ngân hàng kia. Sự chậm trễ này xảy ra do khi bạn thực hiện một giao dịch, mỗi ngân hàng cần một khoảng thời gian nhất định để đối chiếu với sổ cái trung tâm và hệ thống trung tâm của chính ngân hàng đó; chính vì thế, dù ngân hàng này đã ghi nhận rằng giao dịch của bạn đã được gửi đi, ngân hàng kia vẫn chưa xác nhận khoản giao dịch đó đã đến.

Bitcoin sử dụng sổ cái chung, phi tập trung để lập hồ sơ giao dịch, từ đó giúp hoạt động lưu trữ trở nên minh bạch. Mọi người đều có quyền truy cập cùng một thông tin, sổ cái không chịu kiểm soát của bất kỳ một tổ chức riêng lẻ nào cả. Tất cả các giao dịch xảy ra trên

cùng một sổ cái đều được chia sẻ với tất cả mọi người trong mạng lưới.

Trong ví dụ chuyển tiền giữa các ngân hàng khác nhau, giao dịch đó được ghi nhận trên nhiều sổ cái, với mỗi ngân hàng duy trì sổ cái và hệ thống riêng biệt của họ. Với Bitcoin, thay vì các ngân hàng ghi lại các giao dịch trên nhiều sổ cái tập trung, tất cả các giao dịch đều được ghi chép trên một sổ cái phi tập trung cho phép hoạt động tất toán giao dịch gần như tức thời.

Các cơ sở dữ liệu tập trung đã phải hứng chịu rất nhiều vụ tấn công, thao túng, cùng với nguy cơ trộm cắp dữ liệu từ cả bên ngoài và bên trong. Trong lịch sử đã xảy ra trường hợp nhân viên tại các tổ chức tài chính gian lận, đánh cắp ngân quỹ của khách hàng và khiến tổ chức tài chính sụp đổ.

Cơ sở dữ liệu phi tập trung không có hệ thống đơn lẻ nào dễ bị tấn công hoặc thao túng. Bởi vì để thao túng được mạng lưới Bitcoin, cần phải kiểm soát đồng thời hơn 50% máy tính trong mạng lưới, mà điều này gần như là không thể. Tất cả mọi người trên mạng lưới đều có một bản sao của sổ cái, nên dù một máy tính bị tấn công hoặc bị sập cũng không ảnh hưởng đến tất cả máy tính còn lại trong mạng lưới.

Không chịu sự kiểm soát của chính phủ hay ngân hàng

“Không ai quan tâm đến các tình huống quá quắt cho đến khi chúng trở thành một thứ đáng quan tâm”.

- Marc Hochstein

Đặc điểm phi tập trung cùng với việc loại bỏ các tổ chức trung gian sẽ dẫn tới việc không còn chịu sự kiểm soát của chính phủ hay ngân hàng. Điều này làm cho các khoản tiền, tài khoản và giao dịch tài chính thoát khỏi vòng kiểm soát của chính phủ và ngân hàng, và trao quyền cho các cá nhân.

Như đã đề cập ở phần đầu cuốn sách, trong trường hợp của Zimbabwe, chính phủ đã in rất nhiều tiền, và sau đó đồng tiền Zimbabwe đã mất giá đến mức bị coi là vô giá trị.

Tại những đất nước như Zimbabwe, việc chính phủ kiểm soát nguồn cung tiền cũng ảnh hưởng lớn đến người dân. Bởi vì chính phủ hoặc ngân hàng có thể đóng băng tài khoản, thu giữ vốn, hạn chế thanh toán và theo dõi các giao dịch của bạn.

Dù bạn có thể không quan tâm đến việc chính phủ hay ngân hàng nắm quyền kiểm soát, bởi vì bạn không sống ở những quốc gia coi đây là một vấn nạn. Nhưng sự kiểm soát của chính phủ và ngân hàng không chỉ là mối quan tâm ở các nước như Zimbabwe. Wikileaks chính là ví dụ điển hình cho việc chính phủ và ngân hàng có thể đóng băng các tài khoản và hoạt động thanh toán của một tổ chức như thế nào. Họ đã có thể duy trì quá trình hoạt động nếu chấp nhận những khoản đóng góp bằng Bitcoin. Và cho dù bạn đồng tình với việc Wikileaks chia sẻ dữ liệu tuyệt mật của chính phủ hay không, thì đây cũng là một bằng chứng cho thấy dù ở Mỹ và châu Âu không có bất kỳ ai có thể nằm ngoài tầm kiểm soát của chính phủ và ngân hàng.

Bitcoin hoạt động nằm ngoài các hệ thống tài chính hiện hành, nó chỉ được kiểm soát bởi những người trong mạng lưới, chứ không phải bởi chính phủ hay các tổ chức tài chính. Ví Bitcoin không thể bị đóng băng và các khoản thanh toán bằng Bitcoin không thể bị hạn chế. Ví Bitcoin và các giao dịch còn ẩn danh, nên không thể bị theo dõi hoặc liên kết tới danh tính của bạn.

Không có những khoản thanh toán quốc tế đắt đỏ

Hãy quay trở lại ví dụ minh họa về việc những khoản thanh toán Bitcoin tương tự như gửi email.

Nếu bạn giống hầu hết mọi người, bạn có thể gửi đi rất nhiều email mỗi ngày. Và gửi email cho một ai đó cùng quốc gia cũng không khác gì so với gửi email cho một người ở nước khác.

Bất kể bạn gửi email đó đến nước nào, chúng đều giữ nội dung giống hệt nhau, vì vậy chúng ta phải lo lắng khi gửi email quốc tế nữa. Nhưng việc chuyển khoản quốc tế lại là một câu chuyện hoàn toàn khác nhau, vì khi đó, bạn sẽ phải chịu những khoản phí đắt đỏ, thủ tục chuyển khoản phức tạp và thời gian hoàn thành kéo dài nhiều ngày hoặc nhiều tuần.

Mặc dù các công ty như PayPal đã làm cho hoạt động thanh toán quốc tế trở nên dễ dàng hơn, nhưng vẫn còn những khoản phí và những mức giá quy đổi bất lợi mỗi khi bạn thanh toán quốc tế.

Trong khi đó, thanh toán bằng đồng Bitcoin không khác gì khi bạn gửi tiền cho ai đó cùng thành phố hoặc ở giữa châu Phi. Bạn hoàn toàn có thể thanh toán với cùng một mức phí, và sẽ tốn cũng khoảng thời gian đó để người kia nhận được.

Mặc dù bạn có thể không mấy khi gửi khoản thanh toán đến khu vực ở giữa châu Phi, nhưng đối với hàng tỷ người trên thế giới, đây là bước đột phá trong cách thức họ gửi và nhận thanh toán. Nó cũng mở ra những tiềm năng và cơ hội tiếp xúc với nền kinh tế thế giới và các thị trường tài chính cho hàng tỷ người vốn bị đẩy ra ngoài lề.

Bất cứ ai trên thế giới đều có thể bắt đầu kinh doanh, cung cấp dịch vụ nào đó, và giờ đây, toàn bộ thế giới trở thành khách hàng tiềm năng của họ. Internet cho phép họ truy cập thông tin từ khắp nơi trên thế giới, tuy nhiên, nhiều người vẫn bị ngăn cản tham gia nhận hoặc gửi những khoản thanh toán quốc tế. Vì vậy, với Bitcoin, những người nghèo nhất thế giới, vốn bị loại ra khỏi thị trường tài chính thế giới, có thể trở thành một phần của nền kinh tế toàn cầu với những cách thức tham gia hiệu quả và chi phí tham gia thấp.

Chi phí thấp hơn

Không chỉ cắt giảm những khoản phí thanh toán quốc tế đắt đỏ, tất cả các chi phí giao dịch đều có thể được giảm bớt. Với Bitcoin, không tồn tại phí duy trì tài khoản, không yêu cầu tỷ lệ quy đổi khi chuyển khoản giữa các quốc gia, và mức phí giao dịch rất thấp.

Việc loại bỏ các tổ chức trung gian cùng với việc tất toán các giao dịch trên cùng một sổ cái chung thay vì trên nhiều sổ cái riêng còn làm giảm các chi phí xuống. Mỗi lớp loại bỏ trong giao dịch thông qua việc loại bỏ tổ chức trung gian hoặc sổ cái tư nhân còn giảm đi chi phí liên quan đến lớp đó.

Tăng tốc độ giao dịch

Không chỉ chi phí giảm xuống mà tốc độ giao dịch còn tăng lên đáng kể. Việc loại bỏ các tổ chức trung gian và sổ cái tư nhân cho phép các giao dịch được xử lý với tốc độ nhanh hơn nhiều so với các phương pháp hiện hành.

Như đã đề cập trước đó, với một giao dịch thông thường, khi chuyển tiền từ ngân hàng này sang ngân hàng khác, bạn sẽ thấy khoản tiền đó rời khỏi tài khoản bên này nhưng vài ngày sau vẫn chưa xuất hiện trong tài khoản bên kia.

Đối với các chủ cửa hàng, nhận thanh toán qua thẻ tín dụng cũng tương tự như vậy. Bạn có thể trả qua thẻ tín dụng tại cửa hàng, và giao dịch đó sẽ hiển thị tài khoản của bạn đang trong quá trình chờ xử lý mà khoảng thời gian chờ kéo dài tới vài ngày. Như thế, cửa hàng nơi bạn mua hàng có thể không nhận tiền thanh toán cho đến vài ngày sau khi công ty thẻ tín dụng đối chiếu và sắp xếp các khoản tiền thanh toán.

Trong khi đó, Bitcoin cho phép các giao dịch được xử lý gần như ngay lập tức trong đó bitcoin được gửi đi, nhận về và tất toán cùng một lúc.

Tính minh bạch

Bitcoin mang tới những cải thiện đáng kể về tính minh bạch đối với các giao dịch tài chính và sổ sách kế toán hiện tại.

Trên thực tế có thể xuất hiện trường hợp nhân viên hay giám đốc điều hành của một công ty gian lận sổ sách bằng cách thao túng và che giấu giao dịch. Sau khi điều tra những trường hợp như vậy, các

yếu tố mở đường cho hành vi gian lận dần hé lộ: Sự thiếu minh bạch, vì nhiều người không nhận thức được sự tồn tại của các giao dịch bất hợp pháp đó, hay họ không thực hiện đầy đủ và nghiêm túc các hoạt động kiểm tra giao dịch.

Một trong những lợi ích nổi bật của Bitcoin là tính minh bạch. Vì các giao dịch Bitcoin được thực hiện trên một sổ cái chung, phi tập trung và công khai với tất cả mọi người trong mạng lưới. Các giao dịch đều được kiểm nhận bởi hơn 50% số máy tính trên mạng lưới.

Hãy tưởng tượng những hành vi gian lận sẽ giảm thiểu như thế nào khi hơn 50% nhân viên trong một tổ chức đều thực hiện việc kiểm tra giao dịch đã diễn ra. Hãy tưởng tượng nếu hơn 50% khách hàng của một ngân hàng thực hiện hành động kiểm tra các giao dịch. Sẽ rất khó khăn để tồn tại hành vi gian lận với mức độ giám sát này.

Một khi giao dịch được nhập vào Blockchain Bitcoin, nó sẽ không thể bị thay đổi hoặc xóa bỏ. Với những hệ thống hiện thời, kẻ gian sẽ cố gắng che đậy các dấu vết bằng cách thay đổi hoặc xóa sạch thông tin. Điều này là không thể xảy ra ở Bitcoin, bởi trình tự thời gian của các giao dịch Bitcoin có thể được truy nguyên tới tận khối đầu tiên trên Blockchain.

Tất cả các giao dịch đều diễn ra tức thời và bất cứ tình trạng giao dịch nào cũng đều có thể quan sát thấy trên Blockchain Bitcoin. Khi thanh toán hoặc chuyển khoản ngân hàng bằng cách sử dụng các phương pháp hiện hành, bạn sẽ không biết số tiền đó đã được nhận hay chưa, và bạn sẽ phải theo dõi để chắc chắn khoản thanh toán đã được nhận.

Với Bitcoin, khi bạn gửi đi một giao dịch, bạn sẽ nhận được một tham chiếu giao dịch, bạn có thể nhập tham chiếu giao dịch đó vào công cụ Blockchain Expolorer và quan sát trạng thái của giao dịch theo thời gian thực. Hơn nữa, bạn có thể xem và biết được khi nào khoản thanh toán được nhận hay gặp vấn đề. Trong phần sau của cuốn sách, chúng ta sẽ tìm hiểu cách thức khám phá Blockchain của Bitcoin.

Lòng tin

Hiện tại, khi thực hiện một giao dịch, mọi người đều đặt niềm tin vào tổ chức trung gian với kỳ vọng rằng tổ chức đó sẽ tạo điều kiện thuận lợi cho giao dịch xảy ra. Với Bitcoin, lòng tin này được đặt vào mạng lưới, chứ không phải tổ chức trung gian.

Mạng lưới Bitcoin phi tập trung và tất cả mọi người trong mạng lưới đều có thể xem tất cả các giao dịch đã từng xảy ra. Các giao dịch không thể bị thay đổi hoặc xóa bỏ; do đó, nếu một giao dịch xảy ra, mọi người hoàn toàn có thể xem xét và tra cứu từng chi tiết chính xác của giao dịch đó, cũng như các địa chỉ Bitcoin có liên quan.

Bitcoin cho phép loại bỏ các tổ chức trung gian trong khi vẫn duy trì được lòng tin và mức độ bảo mật trong quá trình giao dịch thông qua cơ chế phi tập trung và minh bạch.

Bảo mật

Bảo mật là một trong những yếu tố chính trong thiết kế của Bitcoin. Có rất nhiều tính năng của Bitcoin cung cấp sự bảo mật rất cao.

Mật mã hóa được sử dụng để bảo vệ ví, địa chỉ, danh tính và các giao dịch. Vì thế, gần như bất khả thi trong việc chiếm lấy khóa cá nhân của ai đó để xâm nhập ví Bitcoin của họ thông qua các phương thức tấn công hiện thời như tấn công theo hình thức dò mật khẩu (Brute Force Attack).

Lưu ý: Tấn công theo hình thức dò mật khẩu xảy ra khi có một máy tính tạo ra rất nhiều dự đoán mật khẩu trong một khoảng thời gian ngắn. Thông thường, việc này được thực hiện bằng cách sử dụng các từ, cụm từ và các con số phổ biến như tên1, tên2, tênđứacon1, tênđứacon2, tênthúcưng1, tênthúcưng2, v.v...

Cấu trúc phi tập trung của mạng lưới Bitcoin đồng nghĩa với việc để điều khiển hoặc kiểm soát một hệ thống, kẻ tấn công sẽ phải kiểm soát đồng thời hơn 50% số máy tính trong mạng lưới, mà đây là việc bất khả thi về mặt tính toán. Trong khi đó, ở các hệ thống theo

mô hình tập trung hiện thời, kẻ tấn công chỉ cần tấn công được một máy chủ tập trung là có thể kiểm soát được toàn bộ hệ thống.

Mặc dù tính bảo mật của mạng lưới Bitcoin không hoàn hảo, nhưng nó mang tới nhiều cải tiến đáng kể với nhiều tính năng bảo mật chưa từng tồn tại hoặc bất khả thi trong các hệ thống theo mô hình tập trung hiện có.

Tổng kết chương 5

Bitcoin mang lại nhiều lợi ích, nhưng cũng còn nhiều nhược điểm. Đối với nhiều người, những bất lợi và rủi ro trong việc sử dụng Bitcoin còn vượt xa lợi ích của nó.

Trong chương tiếp theo, chúng ta sẽ cùng tìm hiểu một số rủi ro và bất lợi của Bitcoin.

Chương 6Rủi ro và bất lợi của Bitcoin

“Hãy tránh xa nó. Về cơ bản, nó chỉ là ảo ảnh... Theo quan điểm của tôi, ý niệm cho rằng nó có giá trị nội tại to lớn chỉ là một trò đùa.”

– Warren Buffett

Trong chương trước, chúng ta đã đề cập đến rất nhiều lợi ích của Bitcoin. Với công nghệ mới, thật dễ bị cuốn vào những đồn đại thổi phồng mà chỉ tập trung vào các khía cạnh tích cực của nó. Mặc dù Bitcoin mang lại nhiều lợi ích hơn phương thức thanh toán hiện tại, nhưng đối với nhiều người, có những rủi ro và nhược điểm khiến nó trở nên bất lợi hơn so với cách thức hiện có.

Trong chương này, chúng ta sẽ xem xét một số những rủi ro và bất lợi của Bitcoin.

Phí giao dịch

Khi Bitcoin được tạo ra, các giao dịch đều miễn phí. Đây là một trong những điều hấp dẫn lớn của Bitcoin, khi mà các giao dịch quốc tế có thể được thực hiện miễn phí. Ban đầu, các thợ đào thêm được khối mới vào Blockchain Bitcoin sẽ nhận được phần thưởng khối. Điều này ban đầu là đủ để giúp các thợ đào luôn giữ được nhiệt huyết đóng góp công suất tính toán và nguồn lực để vận hành mạng lưới.

Khi Bitcoin đã dần trở nên nổi tiếng, số lượng thợ đào cạnh tranh giành phần thưởng khối tăng lên, trong khi đó phần thường khối lại giảm theo thời gian và độ khó của Bằng chứng Xử lý cũng tăng cao. Các thợ đào nhận được phí giao dịch của bất cứ giao dịch nào họ thêm vào khối trên Blockchain.

Mặc dù bạn vẫn có thể truyền gửi giao dịch không bị tính phí trên mạng lưới Bitcoin, nhưng chúng sẽ không được ưu tiên hơn so với các giao dịch khác. Bởi vì giao dịch không có khoản phí đi kèm sẽ rơi vào cuối danh sách các giao dịch mà thợ đào lựa chọn, từ đó làm tăng thời gian hoàn thành giao dịch đó.

Theo thời gian, đến cùng sẽ không còn phần thưởng khối để cung cấp cho các thợ đào, và họ chỉ nhận được khoản phí giao dịch. Điều này có khả năng dẫn đến việc các khoản phí giao dịch sẽ tăng cao để bù đắp cho việc phần thưởng khối giảm dần và cuối cùng là xóa bỏ hoàn toàn phần thưởng khối.

Không thể đảo chiều giao dịch

Cho đến nay, không hề xuất hiện giao dịch không chính xác trong Bitcoin. Khi bạn truyền gửi một giao dịch, nó không thể bị tranh chấp, thay đổi hay bị đảo chiều.

Nếu ai đó giành được quyền truy cập vào tài khoản của bạn và gửi bitcoin đến một địa chỉ khác, thì không có ngân hàng hoặc tổ chức trung gian nào đưa ra yêu cầu tái kiểm duyệt giao dịch đó hoặc tố cáo nó là hành vi gian lận. Nếu bạn gửi bitcoin đến nhầm địa chỉ, sẽ không có cách nào để đảo chiều giao dịch và số bitcoin đó sẽ mất hẳn.

Nếu bạn gửi tiền qua hình thức chuyển khoản ngân hàng đến nhầm địa chỉ, giao dịch đó hoàn toàn có thể được đảo chiều. Nếu ai đó giành được quyền truy cập vào tài khoản ngân hàng của bạn hoặc thực hiện hành vi lừa đảo đối với bạn, giao dịch có thể rơi vào tình trạng bị tranh chấp. Các giao dịch trái phép trên thẻ tín dụng cũng bị xử lý qua các biện pháp chống gian lận, ngay cả khi không thể đảo ngược được. Nhưng Bitcoin không có các biện pháp bảo mật tương tự như vậy nhằm chống lại hành vi gian lận hoặc sai sót.

Trong các dự án ICO*, xảy ra rất nhiều những trường hợp lừa đảo, trong đó kẻ lừa đảo cung cấp địa chỉ Bitcoin để lừa bitcoin của những người đăng ký tham gia dự án ICO. Mọi người vội vã đăng ký vì sợ mất cơ hội, họ sao chép địa chỉ được cung cấp, nhanh

chóng gửi bitcoin mà không kiểm tra xem địa chỉ đó có chính xác hay không. Sau khi gửi bitcoin đến địa chỉ giả đó, thì họ không có cách nào để hủy bỏ, đảo chiều hay tranh chấp vì giao dịch được xem là đã hoàn thành, và đương nhiên, cũng không có cách nào lấy lại số bitcoin đó nữa.

* ICO (Initial Coin Offering) là một hình thức kêu gọi vốn đầu tư khá phổ biến trong các dự án tiền kỹ thuật số. (BTV)

Chi phí vận hành mạng lưới Bitcoin

Mạng lưới Bitcoin đòi hỏi nguồn lực tính toán và lượng điện khổng lồ để vận hành.

Bitcoin sử dụng thuật toán Bằng chứng Xử lý đòi hỏi các máy tính phải giải đáp một mảnh ghép toán học để chứng minh rằng chúng đang đóng góp công suất tính toán cũng như các nguồn lực cho mạng lưới. Phần lớn lượng điện năng và công suất tính toán đóng góp vào mạng lưới Bitcoin đều dùng để tạo ra những con số ngẫu nhiên nhằm giải đáp mảnh ghép toán học và chứng minh rằng những nguồn lực đã được đóng góp.

Trung bình, một hộ gia đình thông thường tại Mỹ sử dụng khoảng 10.000-12.000kWh điện mỗi năm. Lượng điện năng tiêu thụ này tương đương với lượng điện cần thiết để tạo ra 4 bitcoin với giá trị khoảng 1.000 đô la mỗi đồng.

Giáo sư John Quiggin, thuộc Đại học Queensland ở Úc, đã tính toán rằng mỗi ngày, mạng lưới Bitcoin sử dụng lượng điện lớn tới mức đủ để cung cấp điện năng cả năm cho khoảng 50 hộ gia đình.

Lượng điện năng này sẽ tiếp tục tăng khi ngày càng nhiều người sử dụng Bitcoin. Điều này khiến việc vận hành mạng lưới Bitcoin trên quy mô lớn trở nên bất khả thi và rất tốn kém so với các lựa chọn thay thế khác.

Thiếu khả năng mở rộng

Điện năng và công suất tính toán chỉ là một số hạn chế trong khả năng mở rộng mà mạng lưới Bitcoin đang phải đối mặt.

Số lượng các giao dịch mà mạng lưới Bitcoin có khả năng xử lý là rất nhỏ khi so với các công ty như Visa và MasterCard.

Cứ 10 phút, mạng lưới Bitcoin thêm một khối giao dịch mới vào Blockchain. Và mỗi khối thường chứa ít hơn 2.000 giao dịch, tức là khoảng 3 giao dịch được xử lý mỗi giây.

Với công suất hiện có, mạng lưới Bitcoin có khả năng tăng gấp đôi số giao dịch hiện được thêm vào mạng lưới Bitcoin, tuy nhiên cũng chỉ đạt khoảng 6 giao dịch được xử lý mỗi giây.

Khi Visa tiến hành các cuộc thử nghiệm với IBM về số lượng giao dịch mà mạng lưới Visa có thể xử lý được, kết luận cuối cùng là, mạng lưới Visa có thể xử lý khoảng 20.000 giao dịch mỗi giây. Đây thực sự là một sự khác biệt rất lớn so với 6 giao dịch mỗi giây mà Bitcoin hiện đang xử lý.

Bitcoin cũng không có phương pháp xác định xem một giao dịch có hợp lệ hay không trước khi giao dịch đó được đưa vào Blockchain. Cùng một số bitcoin có thể bị gửi nhiều lần, nhưng các giao dịch sẽ chỉ bị từ chối khi một trong số chúng được thêm vào khối.

Bạn không thể giao dịch lặp chi bitcoin, nhưng nếu bạn có 10 đồng bitcoin, bạn có thể gửi nhiều giao dịch chứa 10 đồng bitcoin đó cho nhiều người khác nhau, và tất cả các giao dịch đều được hiển thị là đang chờ xử lý. Một khi thợ đào thêm thành công một trong các giao dịch đó vào Blockchain Bitcoin, các giao dịch khác sẽ bị từ chối.

Nhiều công ty chấp nhận thanh toán bằng bitcoin, nhưng họ sẽ phải đợi đủ 6 xác nhận cho đến khi chấp thuận một giao dịch là hợp lệ. Tại sao phải là 6 xác nhận? Bởi vì, một xác nhận tương ứng với một khối mới được thêm vào sau khối có chứa giao dịch đó. Cứ mỗi 10 phút lại có một khối mới được thêm Blockchain, tức là mất khoảng 60 phút để giao dịch đó được chấp nhận là hợp lệ.

Nhưng với thẻ tín dụng, ngay khi bạn mua hàng, giao dịch của bạn sẽ được xác nhận hoặc bị từ chối chỉ trong vài giây. Thẻ tín dụng hiện nay hoàn toàn có thể được sử dụng mà không cần phải nạp vào máy, mã pin hoặc chữ ký. Mua sắm bằng thẻ tín dụng trở nên dễ dàng hơn chỉ bằng cách cà thẻ lên một thiết bị có chức năng xác nhận giao dịch gần như ngay lập tức.

Nếu một cửa hàng phải đợi đủ 6 xác nhận hợp lệ trước khi chấp nhận một giao dịch Bitcoin, bạn sẽ phải đợi khoảng một tiếng tại cửa hàng đó trước khi giao dịch được chấp nhận. Mọi người phản đối lập luận này bằng cách đề cập đến sự tồn tại của các thẻ Bitcoin hiện thời có thể được sử dụng trong các cửa hàng để thanh toán như thẻ tín dụng. Tuy nhiên, nhiều trong số này là thẻ ghi nợ Visa, và chúng không sử dụng bitcoin trong giao dịch mà lại bán bitcoin để đổi lấy đô la Mỹ, và sau đó số đô la này được nạp vào thẻ ghi nợ Visa để sử dụng cho giao dịch. Ở đây, giao dịch diễn ra bằng đồng đô la Mỹ có sử dụng mạng thanh toán của Visa, chứ không phải là bằng bitcoin qua mạng Bitcoin.

Trên thực tế, các đồng tiền mã hóa như Litecoin có thời gian giao dịch nhanh hơn, cứ mỗi 2,5 phút lại có khối giao dịch mới được thêm vào mạng Litecoin. Bitcoin không có bất kỳ một kế hoạch nào để giảm bớt thời gian xác nhận khối, và vẫn chưa có sự đồng thuận về hướng đi tương lai và khả năng mở rộng mạng lưới.

Nếu Bitcoin không thể giải quyết được các vấn đề về khả năng mở rộng, nhiều người dự đoán tương lai của Bitcoin sẽ giống như vàng với chức năng là một nơi cất trữ giá trị, chứ không phải là một phương án khả thi để thay thế thẻ tín dụng và các phương thức thanh toán khác.

Minh bạch hơn nhưng thiếu riêng tư hơn

Ví Bitcoin và các giao dịch đều có tính minh bạch vì chúng cho phép mọi người trên mạng lưới Bitcoin đều có quyền xem xét. Tuy nhiên, tính minh bạch này lại đi kèm với việc thiếu tính riêng tư, từ đó khiến nhiều người không thoải mái khi sử dụng nó.

Thông thường, mọi người đều cho rằng, tránh tham gia và bàn luận đến những chủ đề nhất định như tôn giáo, chính trị và tiền bạc là cách ứng xử tốt. Do đó, mọi người sẽ thấy không thoải mái khi người khác biết được họ kiếm được bao nhiêu, nợ bao nhiêu, và số dư tài khoản ngân hàng của họ là bao nhiêu.

Tính minh bạch của Bitcoin đồng nghĩa với mọi người đều có thể xem xét các giao dịch cũng như số dư tài khoản của bất cứ địa chỉ nào trong mạng lưới Bitcoin. Ngay cả khi các địa chỉ đều ẩn danh, bạn vẫn có thể xác định ai là chủ sở hữu địa chỉ Bitcoin nếu nhận được khoản thanh toán từ họ.

Trong các hệ thống ngân hàng hiện có, nếu bạn của bạn gửi tiền cho bạn, bạn sẽ không biết được số dư tài khoản ngân hàng của họ cũng như tất cả các giao dịch mà họ đã thực hiện. Nhưng với Bitcoin, nếu một người gửi tiền thanh toán cho bạn, bạn có thể xem nội dung tất cả các giao dịch đã diễn ra cùng với số dư hiện tại của địa chỉ Bitcoin đó.

Những thông tin chi tiết về các số dư và các giao dịch được công khai với tất cả mọi người trong mạng lưới Bitcoin. Nếu bạn mua sắm tại cửa hàng, nhân viên ở đó có thể liên kết danh tính của bạn với địa chỉ ví Bitcoin, và xem tất cả các giao dịch bạn đã thực hiện. Nếu tài khoản của bạn nhận được các khoản thanh toán định kỳ, mọi người có thể xác định được số tiền mà bạn kiếm được.

Điều này có thể không thoải mái chút nào nếu bạn đang quyên góp hoặc chi trả cho một nhóm cộng đồng hay nhà thờ địa phương. Họ có thể biết được bạn nạp bao nhiêu tiền vào tài khoản của bạn, số dư hiện tại của bạn và so sánh nó với số tiền bạn quyên góp. Họ có thể nghĩ không tốt về bạn nếu khoản đóng góp của bạn tương đối nhỏ so với lượng bitcoin mà bạn có. Họ cũng có thể xác định những nơi bạn chi tiêu, đánh giá bạn dựa trên các khoản thanh toán mà bạn thực hiện, và khiến các thành viên trong cộng đồng thất vọng khi nhìn thấy chúng.

Ngoài ra, nhiều máy tính đóng góp vào mạng lưới Bitcoin nằm ở các quốc gia như Trung Quốc, một nơi mà chính phủ nắm giữ hồ sơ ghi

chép các hành vi vi phạm nhân quyền. Ở đó, các giao dịch giữa mọi người với các tổ chức mà chính phủ Trung Quốc không chấp thuận có thể bị sử dụng để chống lại những người đang định cư hoặc du lịch tại đó.

Không chỉ chính phủ có thể sử dụng những thông tin này, mà lực lượng tội phạm máy tính cũng có thể tấn công hệ thống và đánh cắp chúng. Điển hình như ở Nga và Trung Quốc, nơi có một lượng lớn máy tính đóng góp vào mạng lưới Bitcoin, có tỉ lệ tội phạm máy tính luôn ở mức rất cao. Tại đó, các hacker có thể sử dụng thông tin giao dịch đã được thực hiện với một số công ty hoặc tổ chức để tống tiền hoặc lợi dụng nhiều người.

Có những đồng tiền mã hóa khác có tính riêng tư cao hơn so với Bitcoin. Cũng có nhiều biện pháp tốt hơn để ẩn đi địa chỉ ví điện tử; tuy nhiên, đối với hầu hết những người mới bắt đầu tìm hiểu về tiền mã hóa, họ sẽ chủ yếu sử dụng Bitcoin và các phương thức giao dịch cơ bản.

Bảo mật cao hơn có thể dẫn đến độ an toàn thấp hơn

Bitcoin áp dụng mức độ an ninh và hệ thống mã hóa tiên tiến hơn so với các hệ thống hiện có. Tuy nhiên, đối với nhiều người, những phương pháp này rất phức tạp và khó hiểu. Hậu quả là, những phương pháp này sẽ trở nên kém an toàn hơn so với các phương pháp truyền thống.

Sử dụng một mật khẩu cơ bản cho hầu hết các trang web sẽ không an toàn bằng việc sử dụng khóa cá nhân của Bitcoin. Nếu bạn làm một phép so sánh nhỏ để kiểm tra xem phương pháp nào là an toàn hơn, thì khóa cá nhân của Bitcoin sẽ có mức độ bảo mật hơn gấp nhiều lần. Tuy nhiên, khi thêm yếu tố con người vào quá trình bảo mật, mức độ an toàn của mỗi phương pháp sẽ thay đổi.

Hãy hình dung thế này, bạn có thể nhớ được mã PIN gồm 4 chữ số của thẻ ngân hàng bạn sở hữu, nhớ mật khẩu đăng nhập hầu hết các trang web, tuy nhiên khóa cá nhân của Bitcoin có lẽ quá khó nhớ. Thắc mắc phổ biến trên các diễn đàn trực tuyến về Bitcoin

hoặc tiền mã hóa là: Làm cách nào để cài đặt lại mật khẩu hoặc truy cập lại nếu tôi quên hay làm mất khóa cá nhân? Câu trả lời là, bạn không thể truy cập số bitcoin của mình nếu quên hay mất khóa cá nhân, vì vậy có một gợi ý nhỏ là bạn hãy ghi lại khóa cá nhân của mình lên một tờ giấy. Tuy nhiên, trên thực tế, các ngân hàng luôn khuyên bạn không nên viết ra mã PIN của thẻ ngân hàng. Như thế, việc chép lại khóa cá nhân, để nhớ được nó, bạn đang vô tình khiến nó trở nên kém an toàn hơn rất nhiều so với mã PIN 4 chữ số của thẻ ngân hàng.

Nếu bạn quên mã PIN của thẻ ngân hàng hay mật khẩu Internet Banking, bạn có thể dễ dàng cài đặt lại bằng cách gọi cho ngân hàng hoặc nhắn tin đến số điện thoại hỗ trợ. Trong khi đó, nếu bạn quên hoặc làm mất khóa cá nhân Bitcoin, sẽ không có cách nào tái thiết lập hoặc truy cập lại. Bạn sẽ không thể truy cập được số bitcoin và ví của mình nếu không có khóa cá nhân.

Có vô số các trường hợp mất khóa cá nhân và không thể truy cập được ví Bitcoin của họ. Giá của Bitcoin đã tăng từ dưới 10 cent trong năm 2010 lên hơn 2.000 đô la trong năm 2017. Điều này tương đương với việc 10 đô la bitcoin năm 2010 sẽ có giá trị trên 200.000 đô la vào 7 năm sau. Với sự tăng trưởng đột biến này, thật dễ hiểu vì sao một số người mua vài bitcoin từ những năm trước, rồi bỏ quên và mất luôn khóa cá nhân của họ.

Bởi vì, vào thời điểm họ mua bitcoin, nó không phải là một khoản tiền đáng kể đến mức khiến họ lo lắng chuyện mất còn; nhưng hiện nay, có thể họ đã mất trắng hàng trăm nghìn hay hàng triệu đô la tính theo giá bitcoin. Một trường hợp nổi tiếng là James Howells ở Anh sở hữu 7.500 bitcoin thu được từ những ngày đầu khai thác. Nhưng sau đó, James đã vô tình ném đi ổ cứng có chứa khóa cá nhân và 7.500 bitcoin trong đó, theo giá Bitcoin hiện tại thì khoản tiền ảo đó tương đương với lượng tài sản trị giá hơn 15 triệu đô la.

Giả sử James Howells không thể truy cập vào tài khoản ngân hàng của mình, anh có thể tới ngân hàng, chứng minh danh tính và lấy lại 15 triệu đô la Mỹ. Tuy nhiên, với Bitcoin, sẽ không có ngân hàng, tổ chức tài chính hoặc bên thứ ba nào để anh liên hệ nhằm khôi phục

quyền truy cập. Một khi khóa cá nhân bị mất, tất cả bitcoin kết nối với ví điện tử đó cũng mất theo.

Khi khóa cá nhân mất, bitcoin vẫn còn trong mạng lưới nhưng không ai có thể tiếp cập chúng. Điều này giống như việc James Howells đến ngân hàng, các nhân viên ngân hàng có thể cho anh thấy số dư 15 triệu đô trong tài khoản, nhưng anh không thể tiếp cận số tiền này. Đây là một ví dụ cho thấy tại sao cách thức bảo mật của mạng lưới Bitcoin lại có nguy cơ kém an toàn hơn, bởi vì bạn dễ gặp rủi ro mất toàn quyền truy cập ví điện tử cũng như số bitcoin của bạn trong đó.

Chủ sở hữu của khóa cá nhân là chủ sở hữu số bitcoin trong ví mà khóa đó có thể truy cập. Nếu ai đó giành được khóa cá nhân của bạn, thì chính họ, chứ không phải bạn, mới là chủ sở hữu số bitcoin trong ví đó. Nếu có ai đó giành được quyền truy cập tài khoản ngân hàng của bạn, bạn có thể liên hệ với ngân hàng để đóng băng các hoạt động chi trả hay rút tiền từ tài khoản của bạn, tranh chấp khi có bất kỳ giao dịch trái phép nào, sửa đổi mật khẩu và giành lại quyền truy cập tài khoản. Tài khoản ngân hàng của bạn có thể được bảo vệ khỏi những hành vi gian lận, và ngân hàng có thể đảm bảo chống lại giao dịch gian lận nếu có, và thực hiện điều tra đối với các giao dịch trái phép.

Với Bitcoin, chủ sở hữu của khóa cá nhân là chủ sở hữu bitcoin. Điều này giống như việc ai đó truy cập mã PIN dành riêng cho thẻ ngân hàng của bạn, và khi bạn đến ngân hàng để khiếu nại, họ trả lời rằng bất kỳ ai có mã PIN đều là chủ sở hữu số tiền trong tài khoản của bạn. Khóa cá nhân được sử dụng với vai trò chứng thực quyền sở hữu, chứ không phải danh tính của bạn, tương tự như việc ngân hàng trao quyền sở hữu tài khoản cho bất kỳ ai có mã PIN của bạn vậy.

Tất cả các tính năng bảo mật và công nghệ mã hóa tiên tiến được tích hợp vào Bitcoin có xu hướng khiến người dùng phải chép lại mật khẩu, và nếu họ làm mất hoặc bị trộm tờ thông tin ghi mật khẩu, họ sẽ không thể cài đặt lại mật khẩu và mất trắng số bitcoin họ sở hữu. Như đã đề cập ở phần đầu nội dung thảo luận này, các lớp

bảo mật bổ sung lại dễ dẫn đến tình trạng kém an toàn hơn cho hầu hết mọi người.

Sau khi đọc phần này, bạn có thể lo lắng và sợ rằng bạn sẽ mất tất cả bitcoin. Tuy nhiên, chúng ta có nhiều lựa chọn thay thế để tránh đa phần các vấn đề nêu trên, có nhiều lựa chọn ví với nhiều công ty vận hành tương tự các tổ chức tài chính hiện thời. Bạn yên tâm, họ hoạt động với vai trò là người giám hộ khóa cá nhân của bạn, bạn có thể cài đặt lại mật khẩu qua email hoặc điện thoại và liên hệ với dịch vụ khách hàng để nhờ giải đáp và xử lí khó khăn trong trường hợp phát sinh vấn đề nào đó; tuy nhiên, sử dụng dịch vụ của các công ty này sẽ loại bỏ một số lợi ích nhất định của Bitcoin. Sự khác biệt giữa các phương án lựa chọn ví sẽ được đề cập đến trong phần sau của cuốn sách.

Kết quả của toàn bộ các đặc tính bảo mật, phi tập trung và loại bỏ các tổ chức trung gian là, hầu hết mọi người vẫn cảm thấy thoải mái hơn với các tổ chức trung gian, tập trung hiện thời, với các dạng mật khẩu tiêu chuẩn, so với các tính năng bảo mật và công nghệ mã hóa tiên tiến của Bitcoin. Mặc dù công nghệ nền tảng của Bitcoin rất tuyệt vời, nhiều người vẫn muốn hi sinh những lợi ích đó để ủng hộ và ưu tiên những gì họ thấy quen thuộc và thoải mái hơn.

Không có hệ thống kiểm soát tập trung không phải lúc nào cũng tốt

“Trong thị trường tài chính, luôn có cơ chế sửa chữa sau các cuộc tấn công. Nhưng trong Blockchain, không có cơ chế nào để sửa chữa việc đó - người ta phải chấp nhận nó.“

- Robert Sams, sáng lập viên kiêm giám đốc điều hành Clearmatics tại London.

Thiết kế của mạng lưới Bitcoin không cho phép một thực thể nào có toàn quyền kiểm soát mạng lưới. Các thay đổi trong mạng lưới phải được chấp thuận bởi phần lớn các máy tính trong mạng lưới.

Về lý thuyết, đặc điểm này thật tuyệt vời, nhưng trên thực tế, cần tới hàng trăm ngàn người sử dụng phải cùng đồng thuận trong các quyết định.

Những quyết định này không chỉ dựa vào quá trình đề xuất vấn đề, tập hợp ý kiến đồng ý hay phản đối của tất cả những người sử dụng, sau đó đưa ra kết luận cuối cùng thuận theo số đông. Mà ở đây, bất kỳ ai cũng có thể đưa ra một đề xuất đòi hỏi toàn mạng lưới phải quyết định. Có thể,

40% mạng lưới đồng ý đề xuất đầu tiên, 40% khác đồng ý đề xuất thứ hai và 20% còn lại có thể đồng ý nhiều đề xuất khác nhau.

Như thế, sẽ không có bất kỳ sự tiến triển nào cho đến khi đa số thành viên trên mạng lưới đồng thuận với một quyết định, điều này đồng nghĩa với sự phát triển và sự tiến bộ của cả quá trình có thể bị đình trệ suốt nhiều tháng hoặc hơn mà vẫn chưa đạt được sự chấp thuận của đa số. Đa số này có thể chiếm hơn 50% tùy theo các quyết định.

Có một ví dụ tiêu biểu về hai luồng ý tưởng khác nhau cho hướng đi tương lai của mạng lưới Bitcoin. Một đề xuất là Nhân chứng Tách rời (Segregated Witness/SegWit) và còn lại là Bitcoin Unlimited. Không đề xuất nào trong hai đề xuất này nhận được sự ủng hộ của đa số để thực thi những thay đổi mang tính phát triển.

Sự bất đồng này diễn ra khiến thời gian giao dịch của Bitcoin chậm lại và tồn đọng nhiều giao dịch chưa được xử lý. Bitcoin đã bị bỏ lại phía sau các đồng tiền mã hóa khác như Litecoin, khi đồng tiền này có thể thực thi những cải tiến với tốc độ nhanh hơn. Cuối cùng, một phần trong mạng lưới Bitcoin tách ra và tự tạo đồng tiền mã hóa riêng lấy tên là Bitcoin Cash.

Với phần mềm và mạng lưới thanh toán tập trung, các công ty toàn quyền thay đổi và quyết định hướng đi tương lai của phần mềm. Trong khi đó, Bitcoin đòi hỏi sự chấp thuận từ đa số người dùng trong mạng lưới mới có thể thực hiện những thay đổi lớn. Điều này giống như việc Visa hoặc MasterCard không thể thực hiện cải cách

trừ khi đa số chủ thẻ tín dụng đồng ý với nó. Như thế, quá trình diễn ra rất chậm, tốn thời gian và khi không có sự chấp thuận của đa số, nó sẽ trì hoãn sự phát triển của toàn mạng lưới.

Nguy cơ xảy ra tấn công mạng lưới Bitcoin

Không có hệ thống kiểm soát tập trung đồng nghĩa với quyền kiểm soát nằm trong tay của bất cứ điều gì mà đa số các thành viên trong mạng lưới chấp thuận.

Nếu ai đó có quyền kiểm soát hơn 50% công suất tính toán trên toàn mạng lưới, họ có thể điều khiển mạng lưới. Việc kiểm soát trên 50% công suất tính toán của mạng lưới được gọi là tấn công quá bán, mà trong đó người nắm quyền kiểm soát có thể quyết định giao dịch nào hợp lệ, họ cũng có thể đảo chiều giao dịch, từ chối giao dịch và giao dịch lặp chi bitcoin.

Nguy cơ xuất hiện tấn công quá bán trên mạng lưới Bitcoin là thấp, vì chi phí và công suất tính toán cần thiết để thực hiện tấn công cực kỳ lớn. Một lượng lớn công suất tính toán trên mạng lưới Bitcoin được vận hành bởi các nhà kho lớn chứa đầy máy tính tại Nga, Trung Quốc và vài quốc gia khác. Nếu những tổ chức này hợp tác với nhau, họ có thể kiểm soát mạng lưới Bitcoin hoặc các mạng lưới tiền mã hóa có quy mô nhỏ hơn.

Cơ hội để một thực thể kiểm soát 51% mạng lưới Bitcoin rất thấp. Tuy nhiên, các vùng khai thác Bitcoin ở quy mô lớn đủ để kiểm soát công suất tính toán để trì hoãn sự phát triển, ngăn chặn đạt được sự đồng thuận của đa số, và can thiệp để quyết định hướng đi tương lai của toàn bộ mạng lưới.

Công nghệ mới chưa được kiểm nghiệm

Bitcoin còn tương đối mới và vẫn chưa nhận được sự chấp thuận bởi phần đông mọi người. Có nhiều vấn đề về khả năng mở rộng và khả năng bảo mật sẽ được thảo luận trong những phần tiếp theo của cuốn sách.

Bitcoin thực sự mang tính cách mạng và có tiềm năng trở thành một đồng tiền chung cho toàn cầu. Tuy nhiên, mẫu câu “X thực sự mang tính cách mạng và có tiềm năng trở thành Y toàn cầu/vĩ đại” được sử dụng rất thường xuyên cho vô số những ý tưởng mới đã thất bại.

Bitcoin có thể được xem tiên tiến hơn so với phương pháp thanh toán hiện tại, nhưng điều đó không có nghĩa là mọi người sẽ sử dụng nó. Nhiều ưu điểm của Bitcoin chủ yếu có thể áp dụng ở các quốc gia theo chế độ độc tài, ở những nơi mà bộ máy chính phủ vận hành không hiệu quả, hay tại các quốc gia mà đồng tiền nội tệ bị coi là vô giá trị, hay tại những nơi mà hệ thống ngân hàng và hệ thống pháp luật không tồn tại hoặc bị tha hóa, xuống cấp. Đối với những người dân sống ở các nước có hệ thống tài chính và pháp lý ổn định, Bitcoin có vẻ kém thích hợp hơn so với các lựa chọn hiện có.

Càng nhiều người sử dụng Bitcoin, nó ngày càng không có khả năng xử lý được sự gia tăng về lưu lượng sử dụng, dẫn đến tốc độ giao dịch chậm hơn và làm phát sinh nhiều vấn đề khác. Hiện vẫn chưa rõ liệu Bitcoin có thể vượt qua được những vấn đề này hay không, và có khả năng Bitcoin không bao giờ xử lý được các cấp độ giao dịch như của Visa hay MasterCard. Trong khi đó, có những đồng tiền mã hóa khác đang thực hiện những cải tiến nhanh hơn Bitcoin. Cụ thể, một đồng tiền mã hóa khác như Litecoin có thể thay thế Bitcoin để đóng vai trò là một đồng tiền mã hóa chính cho các giao dịch.

Hiện Bitcoin vẫn còn là một công nghệ mới trong mắt mọi người, và có thể vẫn còn tồn tại vô số những vấn đề chưa biết mà nó phải đối mặt trong tương lai. Bitcoin có thể mở rộng và vượt qua được những vấn đề này, hay bị chúng ngăn chặn nên không thể trở thành một lựa chọn thay thế được thẻ tín dụng và các phương thức thanh toán khác, vẫn còn chưa rõ ràng.

Tình trạng thiếu niềm tin và tai tiếng của Bitcoin

Mặc dù Bitcoin đã nỗ lực rất nhiều để thoát khỏi mối liên quan với ma túy và tội phạm, nhưng nó vẫn không thể xóa bỏ hình ảnh đó hoàn toàn.

Một sự kiện gần đây là virus tấn công hệ thống máy tính của Dịch vụ Y tế Quốc gia (National Health Service/NHS) tại Anh. Loại virus này ngăn cản người dùng sử dụng máy tính, trừ khi trả cho những kẻ tạo ra virus một khoản tiền chuộc bằng bitcoin. Tình trạng này đồng nghĩa với việc bác sĩ, y tá và nhân viên bệnh viện không thể truy cập hồ sơ bệnh án và những thông tin quan trọng khác. Điều này có thể gây nguy hiểm đến tính mạng cho nhiều bệnh nhân cần được hỗ trợ khẩn cấp trong thời gian này.

Sự kiện này đã được đưa vào mục tin tức nóng hổi trên trang nhất khắp các tờ báo, Internet và truyền hình ở Anh. Trước vụ tấn công này, công dân Anh có lẽ biết rất ít về Bitcoin, nhưng sau sự kiện này, một quan niệm đã bám rễ trong tâm trí mọi người, khi họ cho rằng Bitcoin được sử dụng bởi bọn tội phạm và khủng bố - những kẻ đòi tiền chuộc bằng bitcoin.

Khi sự kiện như thế xảy ra, nó tạo nên ấn tượng mạnh mẽ lâu dài về Bitcoin trong tâm trí công chúng. Và nhìn chung, để mọi người chấp nhận Bitcoin sau những sự kiện như thế này rất khó, bởi vì họ tin rằng họ đang thực hiện những hành động phạm tội bằng cách sử dụng bitcoin, và có nguy cơ dính dáng hay tương tác với bọn tội phạm cùng trong mạng lưới.

Niềm tin kết hợp với danh tiếng cần rất nhiều thời gian xây dựng. Mỗi sự cố về tội phạm liên quan đến Bitcoin đã phá vỡ lòng tin của mọi người và để lại cho họ một ấn tượng tiêu cực sâu đậm.

Thất bại trong việc đạt được sự hiểu biết và công nhận từ công chúng

Để có được sự chấp thuận và khiến cho công chúng chấp nhận sử dụng, mọi người cần phải có niềm tin vào mạng lưới Bitcoin. Bên cạnh đó, họ cũng cần có hiểu biết nhất định và nhận thức được nhu cầu sử dụng bitcoin. Đa số người dân ở Mỹ và châu Âu thường không có nhu cầu về Bitcoin khi so với các phương thức thanh toán hiện tại.

Ngoài ra, những ưu thế của Bitcoin, chẳng hạn như hệ thống mã hóa và sự bảo mật tiên tiến, cũng như khả năng loại bỏ các trung gian giao dịch, không phải lợi ích đối với hầu hết mọi người. Khi lập ví Bitcoin, những thắc mắc đầu tiên mà mọi người thường đặt ra là:

“Tôi phải làm gì nếu mất khóa cá nhân?”

“Làm thế nào để tôi thiết lập lại mật khẩu nếu quên mất nó?”

“Điều gì xảy ra nếu tôi gửi một giao dịch đến nhầm địa chỉ?”

“Tôi có thể liên lạc với ai nếu phát hiện thấy trong tài khoản của mình xuất hiện giao dịch trái phép?” “Tôi có thể liên lạc với ai để thu hồi giao dịch? Đáp án cho những câu hỏi trên là:

• Họ sẽ mất quyền truy cập bitcoin nếu mất hoặc quên khóa cá nhân.

• Các giao dịch không thể bị đảo chiều.

• Nếu họ gửi tiền nhầm địa chỉ, họ sẽ mất tiền.

• Không có công ty nào để liên hệ, vì không có công ty nào chịu trách nhiệm với số bitcoin trong tài khoản của họ.

Nhiều người coi những đáp án này là bất lợi, chứ không phải ích lợi, và làm họ không mấy hứng thú với việc sử dụng Bitcoin:

Việc tìm hiểu về các khóa cá nhân và cách thức Bitcoin hoạt động bị nhiều người coi là chuyện quá phức tạp. Những lợi ích mà Bitcoin đem lại không phải lợi ích dành cho tất cả mọi người, đặc biệt là ở các quốc gia ổn định, và được kiểm soát chặt chẽ bởi hệ thống pháp luật. Ví dụ, nhiều người coi việc loại bỏ các tổ chức trung gian là một bất lợi vì họ muốn biết tiền của họ được các công ty lớn do pháp luật kiểm soát trông coi cẩn thận, mà họ có thể liên lạc tìm trợ giúp nếu cần.

Hiện Bitcoin vẫn chưa được chấp nhận và sử dụng trên quy mô lớn. Mặc dù có nhiều cửa hàng và trang web chấp nhận Bitcoin, nhưng

đó vẫn chỉ là một thị trường người tiêu dùng nhỏ có hiểu biết về công nghệ Bitcoin. Nhìn chung, các bậc cha mẹ sẽ lập ví Bitcoin và chi tiêu bitcoin tại Walmart hay không vẫn còn là một chuyện rất mơ hồ.

Quy định cho Bitcoin và quá trình tích hợp Bitcoin vào hệ thống hiện hành

"Các chuyên viên phân tích và tay chơi tài chính tài năng nhất thế giới đang bàn tán sôi nổi về một phát kiến đang phần nào nổi tiếng vì hứa hẹn sẽ đánh bại họ."

- Mike Gault

Bitcoin đang phải đối mặt với rất nhiều các rào cản về mặt pháp lý trước khi nó được chấp nhận bởi các tổ chức tài chính và chính phủ trên toàn thế giới.

Có rất nhiều hệ thống cạnh tranh với Bitcoin như Ripple đang hợp tác với các ngân hàng lớn, các tổ chức tài chính và các chính phủ trong việc ứng dụng tiền mã hóa và công nghệ Blockchain.

Các ngân hàng, tổ chức tài chính và chính phủ có vẻ không đón nhận Bitcoin ngang tầm với những lựa chọn thay thế chú trọng vào các định chế và tích hợp với thị trường tài chính hiện tại.

Nhiều công ty, chẳng hạn như Circle và Coinbase đã có thể tự kiến thiết như tổ chức tài chính theo luật định ở các quốc gia mà họ hoạt động. Tuy nhiên, điều này lại khiến Bitcoin trở nên tương tự như các phương thức thanh toán tài chính đang chịu kiểm soát của chính phủ và tổ chức tài chính, và tình trạng này đi ngược lại mục đích chính giải thích sự ra đời của Bitcoin.

Hội đồng Giám sát Sự Ổn định Tài chính (Financial Stability Oversight Counsel/FSOC) tại Mỹ đã bày tỏ lo ngại rằng, Bitcoin và các hệ thống tài chính tương tự dựa trên công nghệ Blockchain, mới chỉ được thử nghiệm ở mức độ quy mô nhỏ. FSOC tin rằng, các thử nghiệm trên quy mô nhỏ này không thể hé lộ những nguy cơ gian

lận ẩn tàng, loại rủi ro chỉ có thể trở nên rõ ràng hơn khi Bitcoin và các hệ thống dựa trên công nghệ Blockchain được sử dụng trên quy mô lớn hơn.

Biến động giá

Khi Bitcoin được tạo ra lần đầu tiên, nó có giá dưới 1 cent, và bây giờ nó có giá trị hơn 2.000 đô la Mỹ. Giá cả của Bitcoin thực sự biến động rất mạnh; trong khoảng thời gian từ năm 2012 đến năm 2013, mức giá đã giảm từ khoảng 1.000 đô la xuống còn 200 đô la.

Trong khi đó, giá của các loại tiền tệ pháp định truyền thống hay các hàng hóa truyền thống như vàng không dao động liên tục, mà nhìn chung chỉ thay đổi nhỏ. Nhưng giá của Bitcoin đôi khi có thể dao động hơn 20% chỉ trong vòng một ngày.

Nhiều người tuyên bố rằng mức giá của Bitcoin sẽ đạt 100.000 đô la Mỹ, trái với quan điểm rằng giá Bitcoin có thể sẽ quay trở lại mức 1 cent.

Sự biến động giá cả của Bitcoin không thể dự đoán được, và mức giá tương lai của đồng tiền này vẫn còn là bí ẩn. Không có gì bảo đảm rằng giá của Bitcoin sẽ vẫn ở mức như hiện tại và không ai chắc chắn rằng nó sẽ được chấp nhận trong tương lai.

Những đồn đại thổi phồng về Bitcoin

Có rất nhiều tài liệu nói về việc Bitcoin sẽ thay đổi thế giới, cải cách chính phủ và xóa bỏ hệ thống ngân hàng hiện thời như thế nào.

Mặc dù Bitcoin là một công nghệ mang tính cách mạng đối với nhiều người trên thế giới, tuy nhiên, nhiều tuyên bố về ảnh hưởng của Bitcoin với thế giới lại quá mức phóng đại.

Khi Internet trong giai đoạn bắt đầu trở nên phổ biến và được nhiều người sử dụng, Alan Greenspan đã gọi sự hứng thú của mọi người về Internet là “sự hưng phấn phi lý”. Và nhiều người cũng đang nói những lời tương tự về Bitcoin và sự kích động xoay quanh nó. Mặc

dù nó cung cấp một giải pháp thay thế các hệ thống tài chính và ngân hàng hiện thời đối với nhiều người trên thế giới, nhưng không có gì đảm bảo nó sẽ dẫn đến sự sụp đổ của các hệ thống tài chính hiện tại.

Hiện nay, đang có nhiều đồn đại thổi phồng về việc sử dụng và chấp nhận Bitcoin, tuy nhiên những người sử dụng Bitcoin chỉ giới hạn trong phạm vi những người tiêu dùng trẻ tuổi và am hiểu về công nghệ. Hiện vẫn chưa rõ liệu Bitcoin có nhận được sự chấp thuận của phần đa số mọi người hay không.

Lợi ích của Bitcoin thường bị thổi phồng quá mức, và sự nổi tiếng của Coinbase, Circle cùng các loại ví giao dịch/ví hỗn hợp dựa trên nền tảng web cho thấy mọi người chấp nhận hy sinh nhiều lợi ích của Bitcoin để đổi lấy phương pháp bảo mật truyền thống của ngân hàng và trên Internet. Như đã đề cập, nhiều ưu thế của Bitcoin không được coi là lợi ích đối với hầu hết mọi người ở các nước có nền kinh tế ổn định với hệ thống tài chính và pháp luật được kiểm soát chặt chẽ.

Tổng kết chương 6

Bất chấp nhiều lợi ích sẵn có, tương lai của Bitcoin vẫn rất mơ hồ. Trong phần cuối cuốn sách, chúng ta sẽ cùng tìm hiểu về tác động và tương lai khả dĩ của Bitcoin.

Lúc này, bạn có lẽ đã hiểu về những lợi ích cũng như bất lợi của Bitcoin. Trong chương tiếp theo, chúng ta sẽ xem xét khía cạnh thực tế trong việc thiết lập ví Bitcoin.

Chương 7Các loại ví Bitcoin

“Bitcoin là thành tựu mật mã học đáng chú ý và khả năng tạo nên những thứ không thể sao chép trong thế giới kỹ thuật số mà nó sở hữu có giá trị vô cùng to lớn.”

- Eric Schmidt, CEO Google

Để truyền gửi hoặc thu nhận bitcoin, trước tiên bạn phải thiết lập ví Bitcoin. Có rất nhiều lựa chọn để thực hiện việc này, mỗi lựa chọn đều có ưu nhược điểm riêng.

Trong chương này, chúng ta sẽ khám phá các lựa chọn khác nhau và cách thức sử dụng chúng.

LƯU Ý QUAN TRỌNG: Hầu hết mật khẩu ví, khóa cá nhân và từ khóa khôi phục mật khẩu đều chỉ được phát hành một lần duy nhất. Nếu bạn không viết lại và sao lưu dự phòng, bạn có thể mất quyền truy cập ví cũng như bitcoin của bạn.

Hãy luôn đảm bảo rằng, bạn đã sao lưu dự phòng mật khẩu, khóa cá nhân và từ khóa khôi phục của ví tại nhiều nơi khi bạn khởi tạo ví.

Đối với hầu hết các ví, không có ngân hàng hay tổ chức tài chính nào mà bạn có thể liên hệ để cài đặt lại mật khẩu hay truy cập tài khoản của bạn.

Mất khóa cá nhân, mật khẩu hay cụm từ khôi phục là một trong những nguyên nhân lớn nhất khiến mọi người đánh mất số bitcoin của họ.

Bạn không nên lưu giữ chúng chỉ trên một máy tính, vì nếu bạn mất quyền truy cập máy tính đó, bạn cũng sẽ mất khóa cá nhân của mình.

Có rất nhiều trường hợp trong đó người ta mua bitcoin từ những ngày đầu khi nó xuất hiện, sau đó bỏ quên, làm mất khóa cá nhân, vô tình bán hay ném máy tính chứa mật khẩu đi, để rồi phát hiện số bitcoin đó có giá trị hàng triệu đô la.

Số bitcoin trị giá 10 đô la khi bạn mua chúng vào năm 2010 sẽ để lại cho bạn một khối tài sản có giá trị hơn 1 triệu đô la ở thời điểm hiện tại, vì vậy thật dễ để thấy rằng có bao nhiêu người sở hữu số bitcoin nhỏ trị giá dưới 50 đô la trong những ngày đầu, rồi bỏ quên nó, và bây giờ mất quyền sở hữu hàng triệu đô la trong tay.

Bạn đã được cảnh báo, vì vậy hãy chú ý đến những điều này.

Ví Bitcoin là gì?

Một ví bitcoin được tạo nên từ ba phần chính:

• Địa chỉ Bitcoin của bạn – Trông giống địa chỉ email, địa chỉ này mang tính công khai và bạn có thể cung cấp nó cho những người muốn có một địa chỉ email như bạn. Tuy nhiên, thay vì gửi email cho bạn, họ có thể gửi bitcoin đến địa chỉ này. Một ví Bitcoin có thể chứa nhiều địa chỉ.

• Khóa cá nhân của bạn – Khóa cá nhân là mật khẩu truy nhập địa chỉ Bitcoin của bạn và số bitcoin được giữ tại địa chỉ đó. Khóa cá nhân chứng minh quyền sở hữu bitcoin của bạn, và cho phép bạn ủy quyền giao dịch và truyền gửi bitcoin từ địa chỉ đó. Bạn cần lưu giữ địa chỉ này an toàn và bí mật, kèm bản sao lưu dự phòng khóa cá nhân ở nhiều nơi khác nhau.

• Tổ chức ủy thác/phần mềm Bitcoin để truy cập ví của bạn – Để giao dịch trên mạng lưới Bitcoin, bạn cần phải truy cập vào nó thông qua tổ chức ủy thác Bitcoin, đây có thể là trang web, phần mềm hoặc một phương thức ủy quyền và khởi tạo giao dịch khác.

Nếu bạn vẫn nhầm địa chỉ Bitcoin với địa chỉ email, những nội dung sau đây sẽ giúp bạn thấy rõ sự khác biệt giữa chúng.

Địa chỉ Bitcoin

Địa chỉ Bitcoin giống địa chỉ email ở điểm: Bạn có thể cung cấp địa chỉ này cho bất kỳ ai muốn gửi email cho bạn.

Nếu mọi người có địa chỉ email của bạn, họ có thể gửi email cho bạn nhưng không thể truy cập email của bạn hoặc mạo danh bạn. Điều này cũng tương tự với Bitcoin: Nếu mọi người có địa chỉ Bitcoin của bạn, họ có thể gửi bitcoin cho bạn nhưng không thể truy cập để trộm cắp hoặc mạo danh bạn trên mạng lưới Bitcoin.

Khóa cá nhân Bitcoin

Khóa cá nhân Bitcoin tương tự như mật khẩu được sử dụng để chứng minh bạn là chủ sở hữu địa chỉ email.

Nếu bạn mất mật khẩu email, mọi người vẫn có thể gửi email cho bạn, và thư đến vẫn nằm trong hộp thư, nhưng bạn sẽ không thể truy cập chúng. Nếu ai đó có mật khẩu của bạn, họ có thể truy cập email của bạn và gửi thư mạo danh bạn.

Khóa cá nhân của Bitcoin cũng tương tự như vậy. Nếu bạn mất khóa cá nhân, mọi người vẫn có thể gửi bitcoin cho bạn nhưng bạn sẽ không thể truy cập chúng. Nếu ai đó có được khóa cá nhân của bạn, họ có thể truy cập bitcoin của bạn, và gửi các giao dịch trên danh nghĩa của bạn.

Tổ chức ủy thác/phần mềm Bitcoin

Tổ chức ủy thác/phần mềm Bitcoin tương tự như việc truy cập hòm thư điện tử thông qua trang web của Gmail hoặc phần mềm Microsoft Outlook để truy cập và gửi thư.

Ngay cả khi bạn có địa chỉ và mật khẩu email, bạn vẫn không thể gửi hoặc truy cập email mà không sử dụng trang web hay phần mềm có kết nối với mạng Internet hay mạng lưới email.

Dù không có phần mềm email, địa chỉ email của bạn sẽ vẫn tồn tại, hộp thư đến của bạn vẫn nhận được thư gửi tới. Bạn cũng có thể xem các email đã nhận từ trước và soạn thảo thư nháp ngoại tuyến. Tuy nhiên, nếu không có phần mềm kết nối với mạng lưới email, bạn không thể gửi email hay đọc email mới.

Điều này cũng tương tự với Bitcoin, địa chỉ bitcoin của bạn vẫn tồn tại và bạn vẫn nhận được bitcoin. Bạn có thể sử dụng địa chỉ và khóa cá nhân để tạo giao dịch ngoại tuyến thủ công. Tuy nhiên, nếu không có phần mềm/tổ chức ủy thác Bitcoin có kết nối với mạng lưới, bạn sẽ không thể gửi các giao dịch đã khởi tạo khi ở chế độ ngoại tuyến, quan sát số bitcoin mới nhận được và bitcoin của bạn.

Các phương án ví Bitcoin

Hiện có rất nhiều phương án khởi tạo ví Bitcoin, với số lựa chọn cứ đều đặn tăng lên mỗi tuần. Do vậy, bạn có thể bị choáng ngợp trước toàn bộ những lựa chọn và sự khác biệt giữa chúng.

Tại một hội nghị về tiền mã hóa gần đây, tôi đã gặp những người mà họ đã tải xuống tất cả các loại ứng dụng và phần mềm ví khác nhau, nhưng vẫn chưa tham gia mua bất kỳ bitcoin nào, bởi họ không biết dùng ví nào là tốt nhất. Họ đã tìm hiểu tất cả các thông tin về ví và lo lắng về tình trạng an ninh hoặc nguy cơ mất trộm nếu chọn sai. Quá nhiều thông tin và phương án lựa chọn khiến họ không thể đưa ra được quyết định cuối cùng.

Chương này sẽ bao gồm nhiều tùy chọn khác nhau hiện có. Tuy nhiên, để tránh làm bạn bị chóang ngợp trước các phương án và quyết định, chúng ta sẽ mở đầu bằng những lựa chọn tốt nhất cho người mới bắt đầu với mỗi tùy chọn tăng tiến theo mức độ kinh nghiệm bắt buộc.

Sàn giao dịch/ví web hỗn hợp

Sàn giao dịch/ví web hỗn hợp là một kết hợp giữa ví Bitcoin chạy trên nền tảng web với sàn giao dịch. Đây là một trong những cách dễ dàng nhất để bắt đầu với Bitcoin dành cho hầu hết mọi người.

Một trong những lợi ích của dạng ví hỗn hợp này là bạn có thể sử dụng các phương thức thanh toán hiện tại như thẻ tín dụng, tài khoản ký gửi ngân hàng hoặc PayPal để truy cập bitcoin gần như ngay lập tức.

Sàn giao dịch/ví web hỗn hợp được pháp luật kiểm soát chặt chẽ hơn nhiều so với các lựa chọn ví khác, vì chúng thường nhận được sự hậu thuẫn từ các công ty lớn với vai trò tổ chức giám sát ngân quỹ của bạn. Chúng còn sử dụng nhiều phương pháp bảo mật tương tự các trang web dịch vụ ngân hàng trực tuyến hiện thời, cùng với dịch vụ hỗ trợ khách hàng và giao diện người dùng thân thiện.

Ưu điểm:

• Thuận tiện – có khả năng thực hiện giao dịch qua phương thức thanh toán hiện tại như thẻ tín dụng và chuyển khoản ngân hàng.

• Dễ sử dụng – Vận hành tương tự như các hệ thống ngân hàng trực tuyến hiện hành, dễ cài đặt và sử dụng mà không cần nhiều sự hiểu biết về kỹ thuật.

• Được kiểm soát chặt chẽ bởi hệ thống pháp luật – Các công ty được điều tiết như một tổ chức tài chính.

• Đáng tin cậy – Cơ chế điều tiết từ chính phủ và quy mô công ty nói chung khiến phương án sàn giao dịch/ví web hỗn hợp trở nên đáng tin cậy hơn so với nhiều lựa chọn khác.

• Bảo mật – Sử dụng nhiều tính năng bảo mật của ngân hàng trực tuyến truyền thống.

• Dịch vụ khách hàng – Dịch vụ khách hàng được cung cấp để hỗ trợ người dùng khi có bất kỳ câu hỏi thắc mắc nào hay vấn đề phát sinh nào xảy ra.

• Ứng dụng trên điện thoại di động – Có ứng dụng trên thiết bị di động cho điện thoại hệ điều hành iOS và Android.

• Có tùy chọn sử dụng ví lạnh – Một số sàn giao dịch/ví web hỗn hợp cung cấp tùy chọn ví lạnh với độ bảo mật cao hơn rất nhiều.

Nhược điểm:

• Bạn cần cung cấp thông tin cá nhân để xác minh danh tính của bạn.

• Các giao dịch được kiểm soát dễ dàng hơn, vì chúng xuất đi từ tài khoản liên kết với danh tính của bạn.

• Sàn giao dịch/ví web hỗn hợp không khả dụng với tất cả mọi người trên thế giới.

• Bạn không kiểm soát khóa cá nhân của bạn.

• Thẻ, phiên bản cập nhật phần mềm/các bản vá lỗi và một số dịch vụ hỗ trợ nhất định có thể không khả dụng.

Tổng kết

Sự kết hợp này đồng nghĩa với cả chức năng của ví điện tử thuần túy và chức năng của một sàn giao dịch thuần túy đều là tốt nhất, mà chỉ là sự thỏa hiệp từ cả hai phía.

Loại ví này chịu sự kiểm soát rất chặt chẽ từ hệ thống pháp luật, và tuân theo nhiều quy định tương tự như ở các ngân hàng truyền thống và các tài khoản tài chính. Loại ví này còn yêu cầu xác minh danh tính của bạn, tức là, không có đặc tính ẩn danh và các giao dịch trên ví có thể bị theo dõi.

Sàn giao dịch/ví web hỗn hợp thiếu nhiều lợi ích được xem là những đặc tính tạo nên sự tuyệt vời của Bitcoin trong mắt nhiều người, chẳng hạn như vai trò một đồng tiền ẩn danh phi tập trung không chịu sự kiểm soát của chính phủ hay các tổ chức tài chính.

Ví di động cho Hệ điều hành iOS/Android

Nếu bạn sở hữu điện thoại thông minh, bạn có thể rất đỗi quen thuộc với hàng loạt các ứng dụng mà bạn có thể cài đặt và sử dụng. Các ứng dụng không chỉ để chơi trò Angry Birds hay đăng ảnh lên Instagram, mà còn có cả ứng dụng ví Bitcoin cho điện thoại.

Ưu điểm:

• Dễ dàng thiết lập và sử dụng – Cài đặt ví di động dễ dàng như tải xuống một ứng dụng từ cửa hàng ứng dụng.

• Thuận tiện – Có thể truy cập qua điện thoại thông minh và đăng nhập tương tự như cách bạn làm với các ứng dụng dịch vụ ngân hàng trên di động.

• Bảo mật – Các ứng dụng chạy trên hệ điều hành Android và iOS cần đáp ứng được các quy định của Google hoặc Apple để được xuất hiện trên cửa hàng ứng dụng, từ đó đảm bảo rằng các ứng dụng đã được kiểm tra và xác thực không chứa mã độc.

Nhược điểm:

• Dễ gặp rủi ro điện thoại của bạn bị trộm cắp hoặc bị mất.

• Loại rủi ro trên sẽ ngày càng nguy hiểm nhiều hơn, nếu bạn không sao lưu dự phòng mã khôi phục bên ngoài điện thoại.

• Có nhiều thủ tục đăng ký cần thực hiện và không ẩn danh như các tùy chọn khác.

• Mặc dù Apple và Google đã thực hiện kiểm tra mã ứng dụng, nhưng vẫn có nguy cơ xuất hiện ứng dụng không đến từ các công ty uy tín, vì vậy hãy cẩn thận trong việc lựa chọn ứng dụng cho mình.

• Nhiều ứng dụng không cho phép bạn mua thêm tính năng trong ứng dụng.

Tóm tắt

Nhìn chung, các ứng dụng di động rất dễ cài đặt và sử dụng. Hơn nữa, việc thiết lập các ứng dụng cho điện thoại rất đơn giản, và giúp bạn cảm thấy dễ dàng trong việc bắt đầu tìm hiểu về công cụ này. Nhiều ứng dụng cũng có phần mềm và trang web, vì vậy bạn có thể truy cập ví của mình từ các thiết bị khác.

Sẽ có nhiều rủi ro khi thiết lập ví trên di động nếu bạn không sao lưu dự phòng khóa cá nhân và mật khẩu trên thiết bị khác hoặc nơi khác. Còn có rủi ro vì xuất hiện các ứng dụng không có nguồn gốc từ các công ty uy tín.

Ví dựa trên nền tảng web

Ví dựa trên nền tảng web là ví Bitcoin có thể được truy cập từ một trình duyệt web kết nối Internet. Chúng tương tự như bất cứ trang web nào khác mà bạn đang sử dụng và đều yêu cầu bạn hoàn thành thủ tục đăng nhập.

Ưu điểm:

• Không đòi hỏi bạn phải cài đặt ứng dụng hay phần mềm nào để sử dụng.

• Có thể được khởi tạo dễ dàng từ bất kỳ trình duyệt web nào.

• Có thể được truy cập từ bất kỳ trình duyệt web nào.

• Việc cập nhật máy chủ và phần mềm được công ty chủ quản thực hiện, và bạn không cần cài đặt phần mềm mới.

• Có thể được khởi tạo mà không cần xác minh danh tính.

Nhược điểm:

• Có nguy cơ làm lộ khóa cá nhân của bạn, nếu kết nối Internet không an toàn hoặc máy tính của bạn bị dính virus.

• Rủi ro về việc trang web hoặc máy chủ bị tấn công.

• Rủi ro về việc bất cứ ai ở bất cứ đâu cũng có thể truy cập ví của bạn nếu họ chiếm được khóa cá nhân của bạn.

• Rủi ro về việc máy chủ hoặc trang web của công ty cung cấp ví dựa trên nền tảng web bị mất kết nối Internet, khi đó bạn không thể truy cập ví của mình.

• Các trang web có thể bị các cơ quan chính phủ hoặc nhà cung cấp Internet chặn.

• Có thể cần tới địa chỉ email trong quá trình thiết lập, từ đó loại bỏ đi một số tính năng ẩn danh.

• Nếu bạn mất khóa cá nhân, sẽ không có cách nào để tiếp cận số bitcoin của bạn.

• Có thể không cung cấp dịch vụ khách hàng hay cơ chế hỗ trợ khi có vấn đề phát sinh.

Tóm tắt

Ví dựa trên nền tảng web rất thuận tiện, dễ dàng thiết lập, và có thể được truy cập từ bất cứ thiết bị nào có trình duyệt web và không cần phải cài đặt bất cứ phần mềm hay ứng dụng nào.

Nhưng cũng có rủi ro về bảo mật liên quan đến trang web và mạng Wi-Fi. Do đó, bạn không nên truy cập loại ví này qua mạng Internet công cộng không an toàn hoặc từ máy tính dùng chung.

Ví phần mềm

Nếu sử dụng máy tính, bạn chắc hẳn đã sử dụng một số chương trình phần mềm. Ngày nay, dù việc sử dụng phần mềm máy tính ít đi, và mọi người dùng các ứng dụng trên điện thoại di động hoặc trang web nhiều hơn, thì hầu hết chúng ta vẫn cần tới máy tính xách tay hoặc máy tính bàn hằng ngày. Loại ví phần mềm này cho phép bạn cài đặt ví Bitcoin ngay trên máy tính cá nhân có kết nối với thiết bị đó.

Ưu điểm:

• Dễ cài đặt – Ví phần mềm có thể được cài đặt trong vòng vài phút bằng cách tải xuống tập tin cài đặt và làm theo các bước được hướng dẫn.

• Dễ sử dụng – Ví phần mềm về cơ bản là thân thiện với người dùng.

• Thiết kế – Ví phần mềm thường được thiết kế hợp lý, từ đó giúp tăng cường khả năng sử dụng và quan sát trên màn hình máy tính lên rất nhiều so với trên màn hình điện thoại di động có kích cỡ nhỏ hơn.

• Tiện lợi – Dễ truy cập từ máy tính cá nhân của bạn, tương tự như cách bạn truy cập bất cứ chương trình phần mềm nào khác.

• Phần mềm được bảo mật trên máy tính của bạn.

• Khóa cá nhân thường được mã hóa trên máy tính, và phần mềm của bạn cũng có thể được bảo vệ bằng các mật khẩu thứ cấp.

• Nhận được sự hỗ trợ từ các nhà phát triển phần mềm và bộ phận dịch vụ khách hàng, nếu có vấn đề phát sinh.

Nhược điểm:

• Việc sao lưu dự phòng khóa cá nhân, mật khẩu và từ khóa khôi phục trên máy tính cá nhân có thể khiến bạn mất toàn bộ quyền truy cập nếu máy tính của bạn bị trộm cắp hoặc hư hỏng.

• Công ty chủ quản phần mềm cũng có quyền truy cập khóa cá nhân của bạn kéo theo nguy cơ về bảo mật nếu có vấn đề phát sinh với phần mềm hoặc với công ty đó.

• Không dễ dàng cài đặt và sử dụng như ví di động hoặc ví web hỗn hợp.

• Phần mềm có thể không được cửa hàng phần mềm của Apple hay Windows chấp nhận, nên sẽ có rủi ro trong việc cài đặt trên máy tính.

• Những thiếu sót trong mã lập trình của phần mềm có thể khiến cho nhiều người có quyền truy cập bitcoin của bạn.

• Khóa cá nhân có thể bị công khai nếu được mã hóa không tốt trên máy tính.

• Nếu ví chỉ cung cấp một phiên bản phần mềm thì bạn không thể truy cập vào bitcoin hoặc ví từ điện thoại hoặc qua trình duyệt web.

• Nếu bạn giữ nhiều loại tiền mã hóa trong cùng một ví, thì một người giành được quyền truy cập ví sẽ có khả năng tiếp cận tất cả các loại tiền mã hóa của bạn.

• Phần mềm có thể không được cửa hàng ứng dụng dành cho hệ điều hành Mac OS hay Win- dows chấp nhận, và có thể yêu cầu bạn thay đổi thiết lập bảo mật để vận hành.

• Có nguy cơ bị dính virus nếu bạn không cài đặt từ trang web của công ty chủ quản phần mềm.

• Rủi ro về lỗ hổng phần mềm nếu không được cập nhật phiên bản mới nhất định kỳ.

Tóm tắt

Nhìn chung, ví phần mềm có thể là một lựa chọn tốt, nếu bạn muốn truy cập ví Bitcoin từ máy tính cá nhân thay vì từ ứng dụng di động hoặc từ trang web.

Một số ví phần mềm có thể được liên kết với cùng ví di động và ví dựa trên nền tảng web, từ đó cho phép bạn truy cập ví Bitcoin qua nhiều thiết bị.

Ví phần mềm đòi hỏi người sử dụng phải có kiến thức về cài đặt và thiết lập phần mềm trên máy tính. Điều này nghe có vẻ đơn giản,

nhưng vì phần mềm có thể không được các cửa hàng ứng dụng dành cho hệ điều hành Mac OS hoặc Windows chấp nhận, nó có thể yêu cầu người dùng phải thay đổi chế độ thiết lập bảo mật trong máy tính mới có thể vận hành được.

Hãy cẩn thận khi tải xuống và cài đặt ví phần mềm, đảm bảo rằng bạn đã chọn ví được nhiều người sử dụng và biết tới, và tải trực tiếp từ trang web của công ty chủ quản. Đừng tải từ trang web của bên thứ ba, vì đôi khi các trang web đó có thể đưa phần mềm khác hoặc virus vào gói cài đặt dành cho bạn.

Cuối cùng, hãy nhớ sao lưu dự phòng mật khẩu, khóa cá nhân và cụm từ khôi phục trên một thiết bị khác ngoài máy tính cá nhân mà bạn cài đặt ví phần mềm trên đó.

Sàn giao dịch

Sàn giao dịch hoạt động tương tự như thị trường chứng khoán, trên đó mọi người giao dịch nhiều loại đồng tiền mã hóa cho nhau. Sự biến động giá của Bitcoin và các đồng tiền mã hóa nói chung rất cao, vì vậy mọi người có thể kiếm được rất nhiều tiền chênh lệch hay thua lỗ nhanh chóng.

Ưu điểm:

• Cho phép bạn giao dịch nhiều loại tiền mã hóa với mức phí thấp.

• Thông thường có thể được thiết lập mà không cần quy trình xác minh.

• Nhiều loại tiền mã hóa có thể được lưu giữ trong cùng một tài khoản.

• Có dịch vụ hỗ trợ khách hàng để giải đáp bất cứ câu hỏi và vấn đề nào phát sinh.

• Không yêu cầu phần mềm hay ứng dụng.

• Có thể truy cập từ bất kỳ trình duyệt web nào.

• Các phương pháp bảo mật truyền thống tương tự như dịch vụ ngân hàng trực truyến.

• Mật khẩu có thể được đặt lại nếu bạn quên.

Nhược điểm:

• Yêu cầu địa chỉ email và các thông tin nhận dạng khác trong quá trình thiết lập tài khoản, ngay cả khi bạn chỉ sử dụng tiền mã hóa.

• Bạn sẽ không được ẩn danh và phải cung cấp giấy tờ tùy thân để xác minh danh tính nếu muốn nạp tiền vào tài khoản bằng đồng đô la Mỹ, euro hay loại tiền tệ nào khác.

• Không được thiết kế dành cho các giao dịch mua bán hàng hóa/dịch vụ thông thường, không được dùng để truyền gửi hay thu nhận các giao dịch thông thường từ ví trên sàn giao dịch hoặc cho các dự án ICO.

• Không khả dụng với tất cả mọi người trên thế giới.

• Có nguy cơ mất tất cả ngân sách giao dịch tiền mã hóa vì mục đích đầu cơ kiếm lời.

• Nếu nạp tiền tệ pháp định vào tài khoản, tài khoản của bạn sẽ được kiểm soát tương tự như các tài khoản giao dịch tài chính khác, và có nguy cơ bị đóng vĩnh viễn hoặc thu hồi nếu làm trái với các điều khoản về dịch vụ.

• Bạn không toàn quyền kiểm soát khóa cá nhân của mình.

• Dễ gặp rủi ro với các công ty phức hợp có quy mô nhỏ hơn hoặc được điều tiết lỏng lẻo hơn, nếu họ kiểm soát số dư tài khoản và khóa cá nhân của bạn, điển hình như trường hợp sàn giao dịch Mt. Gox bị phá sản vào khoảng năm 2013 khiến nhiều khách hàng mất trắng.

Tóm tắt

Các tài khoản trên sàn giao dịch không được thiết kế để sử dụng ví dùng cho các giao dịch hằng ngày hay truyền gửi bitcoin. Chúng được thiết kế để được người dùng nạp tiền pháp định hoặc tiền mã hóa để sử dụng cho hoạt động giao dịch định kỳ nhằm đầu tư kiếm lời dựa trên sự biến động giá.

Các sàn giao dịch cho phép bạn nắm giữ nhiều loại tiền mã hóa trong cùng một tài khoản. Họ cũng cung cấp nhiều tiện ích tương tự như những tiện ích của loại sàn giao dịch/ví web hỗn hợp, chẳng hạn như dịch vụ khách hàng, khả năng hỗ trợ và phương thức bảo mật truyền thống.

Bạn không toàn quyền kiểm soát khóa cá nhân trên một sàn giao dịch, tuy nhiên, bạn có thể đặt lại mật khẩu và dễ dàng truyền gửi bitcoin tới các ví khác.

Có rất nhiều rủi ro liên quan hoạt động giao dịch tiền mã hóa.

Tiện ích mở rộng trên Chrome

Tiện ích mở rộng trên Chrome là một ứng dụng nhỏ có thể được cài đặt trong trình duyệt web Chrome của Google. Có hàng ngàn tiện ích mở rộng của Chrome hoạt động với nhiều chức năng đa dạng. Bạn có thể cài đặt tiện ích mở rộng của Chrome, và sử dụng như những ví bitcoin.

Ưu điểm:

• Dễ dàng truy cập bất cứ khi nào bạn đang trực tuyến.

• Tích hợp với trình duyệt web của bạn.

• Cung cấp nhiều cải tiến cho hoạt động lướt web và hoạt động truyền gửi bitcoin – các tiện ích mở rộng của Chrome có thể tìm kiếm địa chỉ bitcoin trên các trang web, từ đó giúp hoạt động truyền gửi bitcoin trở nên dễ dàng hơn.

• Kết nối với Blockchain thông qua trình duyệt.

• Một số tiện ích mở rộng có thể lưu giữ được nhiều loại tiền mã hóa.

• Phần mềm và các ứng dụng dành cho thiết bị di động có thể có tiện ích mở rộng trên Chrome, cho phép bạn truy cập ví từ nhiều nền tảng công nghệ khác nhau.

Nhược điểm:

• Các rủi ro về bảo mật – Mọi người đều có thể tạo tiện ích mở rộng trên Chrome và phát hành trên cửa hàng Google Chrome trực tuyến. Hơn nữa, nhiều tiện ích mở rộng trên Chrome được tạo ra bởi các cá nhân, vì thế có rủi ro về bảo mật nếu các cá nhân đó có quyền tiếp cận khóa của bạn hoặc các trang web bạn đã truy cập.

• Các rủi ro về quyền riêng tư – Các tiện ích của Chrome có thể đọc dữ liệu từ các trang web mà bạn đang truy cập cùng với dữ liệu mà bạn nhập vào trên các trang web đó.

• Chỉ có thể cài đặt chúng trên trình duyệt web của bạn, nên khá bất tiện nếu bạn không thể truy cập máy tính hay trình duyệt đó.

Tóm tắt

Các tiện ích mở rộng của Chrome cung cấp cách tiếp cận ví Bitcoin/tiền mã hóa một cách dễ dàng, vì luôn sẵn có trên trình duyệt Chrome của bạn. Chúng không cung cấp bất kỳ lợi thế nào khác với các lợi ích khi bạn sử dụng phần mềm hay ứng dụng, mặc dù bạn có thể gặp đôi chút khó khăn hơn khi cài đặt và sử dụng. Chúng cũng tạo ra những nguy cơ lớn hơn về bảo mật, so với hầu hết các lựa chọn khác, bởi vì bất cứ ai cũng có thể dễ dàng tạo ra một tiện ích mở rộng trên Chrome.

Các tiện ích trên Chrome có thể là một sự bổ sung tốt cho các tài khoản hiện có vì chúng cho phép bạn truy cập tài khoản từ trình duyệt, nhưng lại không phải lựa chọn tốt nhất đối với hầu hết mọi người.

Ví giấy

Ví giấy là một mảnh giấy với khóa công khai và khóa cá nhân trên đó, giúp bạn truy cập ví Bitcoin. Hầu hết các ví giấy sẽ chứa các khóa công khai/ khóa cá nhân dưới hình thức mã QR*.

* Mã QR (Quick response), tạm dịch là mã phản hồi nhanh hay mã vạch ma trận, là dạng mã vạch hai chiều có thể được đọc bởi một máy quét mã vạch hay điện thoại thông minh có chức năng chụp ảnh với ứng dụng chuyên biệt để quét mã vạch.

Ưu điểm:

• Bảo mật – Khóa cá nhân không được lưu trữ dưới hình thức điện tử.

• An toàn – Không có máy tính hay máy chủ nào có thể tấn công ví giấy của bạn.

• Không có kết nối với mạng Internet và mạng lưới Bitcoin – Ví giấy sẽ không bị ảnh hưởng bởi những lỗi từ máy chủ.

• Một phương án kho lạnh để lưu trữ bitcoin đã được lấy khỏi mạng lưới.

• Ví giấy có thể được nhập vào các ứng dụng khác khi không còn cần thiết.

• Dễ dàng mang theo bên người – Ví giấy có thể được đặt trong sách vở, sổ ghi chép, ví tiền thông thường.

Nhược điểm:

• Dễ bị mất do đãng trí hoặc sơ suất – Bạn rất dễ quên nơi bạn đã cất ví giấy, hoặc đánh mất ví ở đâu đó.

• Dễ bị trộm cắp – Người khác có thể dễ dàng lấy mất ví giấy của bạn mà không cần truy cập máy tính hay máy chủ nào. Thậm chí, ai đó có thể chụp lại ảnh ví giấy của bạn, và lấy trộm bitcoin của bạn.

• Dễ bị phá hủy – Giấy và mực in trên đó có thể bị phai mờ, dễ bị hủy hoại bởi nước, lửa và dễ bị rách.

• Không thể truy cập trên các thiết bị khác, trừ khi các khóa cá nhân và ví được nhập vào ứng dụng.

Tóm tắt

Việc tạo ví giấy và giữ trong tay có thể đem lại cảm giác thú vị, đồng thời cung cấp tính năng bảo mật, giúp bạn tránh được các cuộc tấn công của tin tặc và nhiều vấn đề liên quan đến máy chủ.

Ví giấy không được khuyến khích cho những người mới bắt đầu tìm hiểu Bitcoin, bởi khá nặng tính kỹ thuật, và bạn vẫn cần có tài khoản khác để giao dịch và truyền gửi bitcoin vào ví giấy.

Một điều quan trọng nữa là hãy tìm cách làm cho ví giấy bền hơn nếu bạn có ý định lưu trữ bitcoin trong đó lâu dài, đồng thời cất giữ các bản sao lưu ví ở các vị trí an toàn khác nhau.

Ví giấy dễ bị mất mát, hư hỏng hoặc trộm cắp nếu chúng không được bảo quản cẩn thận, và các bản sao lưu dự phòng không được lưu trữ an toàn.

Ví phần cứng

Ví phần cứng Bitcoin là một thiết bị điện tử nhỏ cùng kích thước với USB hoặc thẻ tín dụng, được dùng để lưu trữ khóa cá nhân cho ví Bitcoin.

Ưu điểm:

• Bảo mật - Ví cứng sở hữu hàng loạt tính năng cung cấp độ bảo mật cao hơn so với các phương án ví khác.

• Khóa cá nhân không được kết nối với máy tính hoặc Internet.

• Việc ký xác nhận giao dịch được thực hiện bên trong thiết bị bảo vệ khóa cá nhân.

• Nếu ví phần cứng bị mất hoặc bị trộm, ví kỹ thuật số này có thể được khôi phục bằng cách sử dụng khóa cá nhân hoặc cụm từ khôi phục.

• Một số ví phần cứng cho phép sử dụng nhiều khóa cá nhân và nhiều cụm từ khôi phục để ẩn số dư bitcoin lớn nếu người nào đó buộc bạn phải cấp cho họ quyền truy cập bitcoin trên thiết bị.

• Một lựa chọn tuyệt vời để lưu trữ bitcoin trong khoảng thời gian dài.

• Khi không có kết nối với máy tính, bitcoin đang được cất giữ trong kho lạnh, tại đó chúng sẽ được ngắt kết nối với Internet hoặc với mạng lưới.

• Được bảo vệ khỏi nhiều loại virus máy tính mà ví phần mềm và ví dựa trên nền tảng web có thể bị nhiễm.

Nhược điểm:

• Dễ mất hoặc bị trộm cắp, do ví phần cứng có cùng kích thước với chiếc USB hay thẻ tín dụng.

• Nếu ví phần cứng bị mất do sơ suất, đãng trí hoặc bị đánh cắp mà bạn không có bản sao lưu dự phòng từ khóa khôi phục, bạn sẽ mất quyền truy cập bitcoin của mình.

• Dễ dàng bị cơ quan chính phủ tịch thu, nếu bạn truyền gửi bitcoin sang nước khác.

• Một số chức năng có thể được mã hóa cứng, và không thể thay đổi nếu không có kết nối với phần mềm khác, chẳng hạn như việc thiết lập mức phí cho một giao dịch.

• Đắt đỏ hơn so với các lựa chọn khác.

• Rủi ro về ví phần cứng giả với phần mềm độc hại, nếu bạn không mua nó từ một công ty có uy tín.

• Yêu cầu thiết bị phần cứng phải cắm vào máy tính để truyền gửi bitcoin.

• Thuận tiện trong việc lưu trữ bitcoin, nhưng có thể không phải là lựa chọn tốt nhất cho các giao dịch Bitcoin thông thường.

Tóm tắt

Ví phần cứng là một trong những cách an toàn nhất để lưu trữ một số lượng lớn bitcoin. Trong đó, khóa cá nhân của bạn sẽ được bảo vệ, bitcoin được cất giữ trong kho lạnh khi không kết nối với máy tính, nên không có nguy cơ bị lây nhiễm virus như các loại ví khác.

Ví phần cứng chỉ chứa khóa cá nhân, nên miễn là bạn có các bản sao lưu dự phòng hoặc khóa cá nhân và cụm từ khôi phục, bạn vẫn có thể truy cập bitcoin của bạn ngay cả khi ví phần cứng bị mất, hư hỏng hay trộm cắp.

Một số ví phần cứng cho phép sử dụng đa khóa cá nhân và nhiều từ khóa khôi phục, cho phép bạn cung cấp cho ai đó khóa cá nhân và từ khóa khôi phục chỉ truy cập được địa chỉ bitcoin chứa số ít bitcoin hơn trên ví, đồng thời bảo vệ được số dư bitcoin lớn hơn trên thiết bị.

Ví phần cứng là một cách lưu trữ bitcoin an toàn trong dài hạn, nhưng không thuận tiện với các giao dịch bitcoin thường xuyên, vì không phải lúc nào bạn cũng có thể truy cập vào một máy tính cá nhân.

Ví phần cứng cũng có thể không phải là lựa chọn tốt nhất để vận chuyển trên phạm vi quốc tế. Đã có những trường hợp mà lực lượng an ninh sân bay tịch thu ví phần cứng, vì họ không chắc thiết bị này là gì, hoặc khi việc vận chuyển bitcoin xuyên quốc gia bị liệt kê là hành vi phạm pháp.

Ví phần cứng chủ yếu dành cho những người dùng Bitcoin giàu kinh nghiệm, vì vậy nếu bạn là người mới tìm hiểu Bitcoin, tốt hơn hết là

bạn nên cân nhắc một trong số các lựa chọn khác đã được đề cập đến trong chương này trước khi đưa ra quyết định cuối cùng.

Tổng kết chương 7

Nhìn chung, có rất nhiều lựa chọn ví bitcoin, tuy nhiên nhiều trong số chúng không cung cấp cho bạn tính năng mua bitcoin. Mỗi loại ví có những lợi thế và bất lợi khác nhau, và kèm theo đó là những rủi ro nhất định.

Bên cạnh đó, hãy luôn sao lưu dự phòng khóa cá nhân và mật khẩu của bạn trên một thiết bị phần cứng khác. Đặc biệt, hãy nghĩ tới tình huống nếu thiết bị của bạn bị đánh cắp, mất mát, hay hư hỏng khiến bạn không thể truy cập, khi đó bạn sẽ khôi phục ví Bitcoin từ thiết bị phần cứng như thế nào. Sẽ không an toàn nếu bạn lưu khóa cá nhân trên cùng một thiết bị phần cứng được sử dụng như ví điện tử của bạn, vì nếu có chuyện gì xảy ra với thiết bị đó, bạn sẽ mất khóa cá nhân.

Một ví dụ so sánh thực tế đã xảy ra với tôi trong chuyến du lịch lần đầu tiên ra nước ngoài. Khi ấy, tôi giữ một khoản dự phòng cho trường hợp khẩn cấp tại một ngăn bí mật trong ví. Suy nghĩ của tôi khi đó là nếu ai đó dùng vũ lực để cướp chúng, tôi có thể giao cho người đó toàn bộ tiền mặt hiện có, cho họ thấy đó là tất cả số tiền tôi đang sở hữu, và tôi vẫn giữ được khoản dự phòng kia. Tuy nhiên, tôi lại không nghĩ tới khả năng bị móc túi, mất cả chiếc ví cùng với số tiền dự phòng được giấu trong đó.

Điều này cũng đúng đối với ví Bitcoin, khi khóa cá nhân, cụm từ khôi phục và mật khẩu của bạn sẽ được dùng đến trong trường hợp khẩn cấp. Nếu bạn lưu trữ chúng trên cùng một thiết bị như ví Bitcoin, thì cũng giống như việc bạn lưu trữ chúng trong ví bỏ túi của bạn vậy. Theo đó, nếu thiết bị đó bị mất cắp, kéo theo toàn bộ ví của bạn, và bạn sẽ mất toàn bộ số tiền hiện có cũng như số tiền dự phòng trong đó.

Hãy học hỏi từ những sai lầm của tôi và nhớ sao lưu dự phòng khóa cá nhân, mật khẩu và cụm từ khôi phục một cách an toàn tại vị trí

riêng biệt, hoặc trong một thiết bị khác không phải chính ví Bitcoin của bạn.

Chương 8Khám phá Blockchain Bitcoin

“Trao cho người dùng khả năng truy cập dễ dàng tới nhiều loại tài sản kỹ thuật số đa dạng trên Blockchain, đặc biệt các phiếu liên kết với tài sản thực, là yếu tố tiên quyết để đưa công nghệ Blockchain lên tầm cao mới…“

- Vitalik Buterin, nhà sáng lập Ethereum

Blockchain Bitcoin là cơ sở dữ liệu của tất cả các giao dịch Bitcoin đã diễn ra kể từ khi Bitcoin ra đời.

Bạn có thể kiểm tra tình trạng giao dịch, xem giao dịch trước đó, xem số dư bitcoin tại địa chỉ ví, và thậm chí có thể tra cứu từ các giao dịch trong quá khứ cho đến giao dịch gần nhất trên Blockchain của Bitcoin.

Có một số trang web khác nhau để khám phá Blockchain Bitcoin, trong đó nổi tiếng nhất là blockchain.info, tại địa chỉ www.blockchain.info.

Trong chương này, chúng ta sẽ tìm hiểu một số yếu tố trong giao dịch Bitcoin, thứ cấu thành nên một khối, cũng như cách thức khám phá Blockchain.

Blockchain Bitcoin

Một khối mới, có chứa một tập hợp các giao dịch Bitcoin, được thêm vào Blockchain Bitcoin cứ mỗi 10 phút một lần. Khi một khối được thêm vào Blockchain, các giao dịch trong khối trở thành một phần của Blockchain.

Khi bạn truyền gửi bitcoin đến địa chỉ Bitcoin khác, giao dịch sẽ ở trạng thái chờ cho đến khi được thêm vào một khối trên Blockchain.

Khối đầu tiên trên Blockchain được gọi là “Khối Nguyên thủy”, nó là khối số 0 trên Blockchain. Khối tiếp theo được thêm vào Blockchain là khối 1, mỗi khối được thêm trên khối 1 sẽ có số thứ tự tăng dần, đây được gọi là chiều cao khối.

Khi một khối được thêm vào Blockchain, nó có sự liên kết với khối liền trước, tức là khối 10 có sự liên kết với khối 9, khối 9 có sự liên kết với khối 8, và cứ tiếp tục như vậy cho đến khối đầu tiên (khối 0) trên Blockchain. Các khối đều có sự liên kết với nhau như một chuỗi, đó là chính lý do cái tên Blockchain (chuỗi các khối) ra đời.

Khám phá Blockchain

Nếu bạn muốn tìm hiểu các nội dung được đề cập lần lượt trong chương này trên một Blockchain thực sự, bạn có thể gõ đường dẫn www.blockchain. info trên trình duyệt web của bạn.

Bạn không cần phải xem tận mắt Blockchain mới hiểu tường tận những thông tin trong chương này, vì vậy nếu bạn hiện không dùng máy tính hoặc chỉ thích tìm hiểu qua việc đọc sách, bạn cũng sẽ không bỏ lỡ thông tin nào.

Trang chủ blockchain.info hiển thị các khối mới nhất được thêm vào Blockchain. Trên đó, trang chủ trình bày các cột với chiều cao khối, tuổi thọ, giao dịch, tổng số đã gửi, người khởi tạo và kích thước khối.

Vào thời điểm viết cuốn sách này, khối mới nhất trên Blockchain là 473609 với các thông tin chi tiết như sau:

Chiều cao khối: 473609 – Đây là số khối trên Blockchain khi khối này được thêm vào. Khối tiếp theo được thêm vào trên khối này sẽ là khối 473610, và khối trước khối này là 473608.

Tuổi thọ: 10 phút – Khoảng thời gian tính từ lúc khối này được thêm vào Blockchain tới thời điểm quan sát.

Giao dịch: 2427 – Số lượng các giao dịch chứa trong khối.

Tổng số đã gửi: 9.958,62 BTC – Số bitcoin được truyền gửi giữa các địa chỉ trong khối này.

Người khởi tạo: Bixin – Thợ đào đã thêm khối 473609 vào Blockchain.

Kích thước khối: 998,183 – Kích thước tập tin khối, hiện các khối bị giới hạn ở mức khoảng 1.000 kb.

Đường dẫn đến chính xác khối này trên Blockchain có tại: www.bitly.com/bitblock1.

Khám phá dữ liệu từng khối

Mỗi khối trên Blockchain có thể được khám phá chi tiết hơn, nếu bạn nhấp vào liên kết trên hoặc bất kỳ khối nào khác trên Blockchain, hoặc tìm hiểu dần dần thông qua nội dung sách.

Khối bên trên có chứa các thông tin sau đây:

Tóm lược

1

Tìm hiểu thông tin trong khối

Có rất nhiều dữ liệu chứa trong mỗi khối, tuy nhiên, nếu không hiểu hết ý nghĩa, những thông tin đó sẽ không giúp ích được gì cho chúng ta.

Chúng ta có thể kiểm tra từng trường thông tin để hiểu thêm về khối 473609, cũng như dữ liệu chứa trong các khối trên Blockchain Bitcoin.

Số lượng giao dịch: Đây là một khái niệm tương đối dễ hiểu, cho biết số các giao dịch Bitcoin có trong khối đó. Khối này chứa 2.427 giao dịch Bitcoin riêng rẽ.

Tổng số đã gửi: 9.595,61973656 BTC

Khối lượng giao dịch ước tính: 601.46273237 BTC Một ví dụ để hiểu về “Tổng số đã gửi” và “Số lượng giao dịch ước tính” là câu chuyện mua một cốc cà phê:

Một cốc cà phê có giá 5 đô la. Bạn trả bằng tờ tiền 20 đô la, thì nhân viên thu ngân sẽ gửi lại cho bạn 15 đô la tiền lẻ. Trong trường hợp của bitcoin, thì tổng số đã gửi của giao dịch này là 20 đô la và khối lượng giao dịch ước tính là 5 đô la.

Cách thức hoạt động này vận hành trong Bitcoin mang nặng tính kỹ thuật nên sẽ không được đề cập chi tiết trong sách, tuy nhiên hàm ý tương tự như trên.

Phí giao dịch: Khi một giao dịch Bitcoin được gửi đi, sẽ có một khoản phí giao dịch nhỏ được tính cho hoạt động truyền gửi giao dịch. Tổng phí giao dịch kết hợp cho tất cả các giao dịch trong khối này là 0,77493411 BTC, có giá trị tương đương vào khoảng 2.000 USD tại thời điểm viết sách.

Các khoản phí giao dịch này được trả cho người thợ đào đã khai thác thành công khối 473609.

Chiều cao khối: Đây là số thứ tự của khối trên Blockchain. Khối này có chiều cao khối là “473609 (Chuỗi chính)”. Đó là khối thứ 473.609 được thêm vào Blockchain Bitcoin tính từ khối đầu tiên.

Khối đầu tiên trên Blockchain Bitcoin có chiều cao khối là 0, tức là đã có 473.609 khối được thêm vào Blockchain của Bitcoin trước khối này.

Nhãn thời gian: Là thời điểm khối được thêm vào Blockchain, khối này đã được thêm lúc 3 giờ, 20 phút, 6 giây ngày 01 tháng 07 năm 2017.

Thời gian nhận: Là thời điểm khối được mạng lưới chấp nhận. Khối này được chấp nhận cùng thời điểm nó được tạo ra, tức là lúc 3 giờ, 20 phút, 6 giây ngày 01 tháng 07 năm 2017.

Người khởi tạo: Mỗi khối được thêm vào Blockchain Bitcoin bởi một thợ đào. Mỗi thợ đào thường là một nhóm các máy tính tổng hợp nguồn công suất tính toán của họ để sử dụng cho Blockchain của Bitcoin. Khối 473609 được thêm vào bởi thợ đào “Bixin”.

Đây có thể là một tên công ty sở hữu công suất tính toán rất lớn dùng cho hoạt động khai thác Bitcoin.

Độ khó: 711.697.198.173,76. Con số này thể hiện độ khó hiện tại của thuật toán Bằng chứng Xử lý mà các thợ đào phải giải quyết để thêm được một khối vào Blockchain. Độ khó được điều chỉnh để đảm bảo các khối được thêm vào Blockchain khoảng 10 phút một lần.

Kích thước: Đây là kích thước tập tin của khối dữ liệu giao dịch. Khối 473609 có kích thước tập tin là 998,183 KB. Giới hạn kích thước tập tin khối hiện tại của Bitcoin vào khoảng 1.000 KB.

Phiên bản: Các thợ đào có thể thêm dữ liệu vào khối này để bỏ phiếu cho các đề xuất về phiên bản phần mềm, dữ liệu trong khối này là 0x20000002, một phiếu bầu cho đề xuất SegWit.

Tham số Nonce: Nonce (Number Used Once) nghĩa là số được dùng một lần, đây là đáp án cho mảnh ghép toán học mà các thợ đào phải giải quyết để thêm được một khối vào Blockchain. Đó là con số được tạo ra ngẫu nhiên, và khi được kết hợp với dữ liệu giao dịch trong khối, nó sẽ tạo ra một mã băm có giá trị thấp hơn băm chỉ tiêu hiện thời của mạng lưới Bitcoin. Tham số Nonce của khối này là 3477743642.

Phần thưởng khối: Đây là phần thưởng khối trả cho thợ đào mỏ đã có công thêm khối đó vào Blockchain. Thợ đào của khối 473609 nhận được 12,5 bitcoin, vào khoảng 30.000 USD tiền thưởng thời điểm bấy giờ.

12,5 bitcoin này là những bitcoin mới được tạo ra. Phần thưởng khối sẽ giảm đi một nửa cho đến khi 21 triệu bitcoin được tạo ra, và

sau đó các thợ đào sẽ chỉ nhận được phí giao dịch cho việc khai thác khối.

Tìm hiểu về mã băm

Khối 473609 còn chứa dữ liệu băm, chính là mã băm của tất cả các dữ liệu giao dịch cùng với tham số Nonce của khối này. Sự thay đổi nhỏ nhất trong bất kỳ dữ liệu nào của khối sẽ dẫn tới việc thay đổi mã băm. Dù chỉ đổi một chữ cái từ viết thường thành viết hoa cũng dẫn đến một mã băm hoàn toàn khác.

Mỗi khối có chứa mã băm của khối trước đó trên Blockchain. Khối liền trước có chứa mã băm của khối trước đó nữa, cứ tiếp tục như vậy cho đến khối đầu tiên, hay còn gọi là "Khối Nguyên thủy".

Điều này giúp liên kết tất cả các khối với nhau thành một chuỗi. Sự kết nối này giúp ngăn chặn các cá nhân và tổ chức thao túng hoặc thay đổi các giao dịch trước đó nhằm trộm cắp bitcoin.

Nếu dữ liệu trong một khối bị thay đổi, nó sẽ thay đổi cả mã băm, dẫn đến khối này không còn liên kết tới khối trước nó và sau nó nữa; hậu quả là toàn chuỗi sẽ bị phá vỡ. Cách duy nhất để thay đổi dữ liệu trong một khối và hợp thức hóa việc này là thay đổi mã băm của toàn bộ các khối trước nó trên Blockchain. Điều này gần như là bất khả thi sau mỗi 6 khối, vì công suất tính toán cần thiết quá lớn.

Mã băm của khối này là:

000000000000000000e589576a954ac - 374d0a98478007a82f2a57f76e243ece3

Mã băm của khối liền trước nó là:

000000000000000000a2591c88266342e - 6f7380a275d5b98e1882f85347c48db

Mã băm của khối liền sau nó là:

00000000000000000642e6876c941bdee8f68e -
c81863e801065b23e4942ad43

Dữ liệu băm của khối tiếp theo được bổ sung bởi công cụ khám phá Blockchain ngay khi khối tiếp theo được thêm vào. Dữ liệu này còn là bí mật vào thời điểm khối này được thêm vào Blockchain.

Rễ cây Merkle

7b67bae1539dce51b404e-
7a153e6de2e39103ef089f4d2b2c74778f85ed7a88a

Cây Merkle là một chủ đề nặng tính khoa học nên sẽ không được đề cập chi tiết trong cuốn sách này. Về cơ bản, trong một khối, mỗi giao dịch đều có một mã băm. Rễ cây Merkle là mã băm của toàn bộ mã băm giao dịch trong khối.

Khám phá các giao dịch

Công cụ khám phá khối cũng sẽ liệt kê chi tiết mỗi giao dịch trong một khối. Bạn có thể đi xa hơn trong việc khám phá Blockchain của Bitcoin bằng cách kiểm tra từng giao dịch trong một khối.

Trong ví dụ về khối, đường dẫn tới một giao dịch nó chứa đựng tại đây: www.bitly.com/blocktran1

Giao dịch này chứa các thông tin được liệt kê dưới đây:

Mã băm giao dịch

35058dc82bb13274236302170d8462aa8030992d-
c30f8e90392f50f96ca8752c

Thông tin giao dịch

2

Tìm hiểu về các giao dịch

Mỗi bitcoin có thể được chia thành đơn vị nhỏ hơn, đơn vị nhỏ nhất là một phần một triệu của bitcoin, được gọi là Satoshi.

Xem dữ liệu giao dịch này, chúng ta có thể thấy rằng 0,03070786 bitcoin đã được gửi từ địa chỉ Bitcoin 1BXrAQukH3EeZJmnSMiSCXuQ5vUe- EQvJbB tới địa chỉ Bitcoin 144neoeit3xA8zXkDU-86VeKNGTD1GqLyA4.

Dữ liệu nhập: Số bitcoin đã được gửi là dữ liệu nhập của giao dịch này: 0,03070786 BTC.

Phí: Mỗi giao dịch của Bitcoin đều có một khoản phí. Phí của giao dịch này là 0,00064636 BTC.

Dữ liệu xuất/Số tiền chưa tiêu dùng: Lượng tiền Bitcoin cuối cùng mà người nhận đã nhận được sau phí, được gọi là số tiền xuất hoặc số tiền chưa tiêu dùng của giao dịch. Trong ví dụ này, con số đó là 0,0300615 BTC.

Số BTC giao dịch ước tính: Đây là giá trị ước tính của giao dịch sau phí, giá trị ước tính của giao dịch này là 0,0300615 BTC, tương đương với giá trị của Dữ liệu xuất/Số tiền chưa tiêu dùng ở trên.

Kích thước: Đây là kích thước của dữ liệu giao dịch, trong ví dụ này, kích thước là 192 byte. Một khối trên Blockchain Bitcoin hiện chứa khoảng 1 triệu byte dữ liệu, xấp xỉ 5.000 giao dịch trong mỗi khối với kích thước giao dịch này.

Thời gian nhận: Đây là thời điểm giao dịch được mạng lưới chấp nhận. Nó đã được chấp nhận vào lúc 3 giờ, 19 phút, 8 giây, ngày 01 tháng 07 năm 2017.

Bao gồm trong khối: Cụm từ này muốn nói đến khối số mà giao dịch này đã được bao gồm trong khối số đó. Giao dịch này đã được bao gồm trong khối số 473609 trên Blockchain Bitcoin. Giao dịch đã được thêm vào Blockchain Bitcoin vào thời điểm (ngày và giờ): 2017/07/01 03:20:06 + 1 phút. Như vậy, giao dịch này đã được thêm

vào khối số 473609 đúng 1 phút sau khi y được chấp nhận bởi mạng lưới.

Xác nhận: Xác nhận là số lượng khối đã được thêm vào Blockchain Bitcoin sau khối có chứa giao dịch này. Một giao dịch càng có nhiều xác nhận, thì càng ít có khả năng bị đảo chiều hoặc bị thay đổi. Trong ví dụ này có 3 xác nhận, nhiều công ty sẽ phải đợi đủ 6 xác nhận trước khi chấp nhận một giao dịch là hợp lệ.

Giao dịch này đã được thêm vào khối 473609, việc đã có 3 xác nhận đồng nghĩa là 3 khối nữa đã được thêm vào sau khối này.

Chúng ta có thể tính toán khối gần đây nhất trên Blockchain Bitcoin bằng cách cộng thêm số xác nhận vào số khối mà giao dịch này chứa trong đó. Tức là thực hiện phép cộng (473609 + 3), chúng ta có thể tính ra rằng, vào thời điểm tôi viết cuốn sách này, Blockchain của Bitcoin chứa khối mới nhất là khối số 473612.

IP người khởi tạo: Mỗi nút tiêu chuẩn trong mạng lưới Bitcoin đều chứa một bản sao Blockchain và các giao dịch. Trong trường hợp này, chúng ta đang xem giao dịch từ bản sao Blockchain được do blockchain.info lưu trữ.

Mô phỏng: Chức năng này cho phép bạn xem cây Merkle, hiển thị dữ liệu nhập của giao dịch và dữ liệu xuất chưa được tiêu dùng của giao dịch này.

Khám phá địa chỉ Bitcoin

Khi quan sát một giao dịch, chúng ta có thể thấy người gửi và người nhận giao dịch. Chúng ta có thể đi sâu vào việc khám phá Blockchain Bitcoin, bằng cách nhìn vào các địa chỉ liên quan trong giao dịch.

Người gửi

Trong ví dụ này, địa chỉ Bitcoin của người gửi là:

1BXrAQukH3EeZJmnSMiSCXuQ5vUeEQvJbB Chúng ta có thể xem địa chỉ đó trên công cụ khám phá Blockchain tại liên kết: www.bitly.com/bitadd1

Địa chỉ Bitcoin của người gửi trên công cụ khám phá Blockchain, hiển thị các thông tin sau:

Giao dịch

3

Chúng ta có thể thấy, có 2 giao dịch trên địa chỉ này, họ đã nhận được tổng số là 0,03070786 BTC và có số dư cuối cùng là 0 BTC.

Chúng ta có thể quan sát các giao dịch đã nhận và nơi nó được gửi đi.

Địa chỉ này ban đầu nhận được 0,03070786 BTC từ địa chỉ ví Bitcoin: 3H5bQN4rhEgryUa1My8KX-eGj4x5Z2irDXV vào lúc 3 giờ 16 phút 7 giây ngày 01/07/2017. Sau đó, họ đã gửi cùng số tiền đó cho người nhận vào lúc 3 giờ 19 phút 8 giây ngày 01/07/2017.

Có vẻ họ đã nhận được số tiền chính xác như yêu cầu, sau đó chuyển nó từ địa chỉ đó tới người nhận vài phút sau đó. Cũng có khả năng họ đang tạo địa chỉ mới cho mỗi giao dịch và cố gắng giữ bí mật các giao dịch và ví của mình.

Người nhận

Trong ví dụ này, địa chỉ Bitcoin của người nhận là:

144neoeit3xA8zXkDU86VeKNGTD1GqLyA4

Chúng ta có thể xem địa chỉ đó trên công cụ khám phá Blockchain tại liên kết: www.bitly.com/bitadd2

Địa chỉ Bitcoin của người nhận trên công cụ khám phá Blockchain, hiển thị thông tin sau:

Giao dịch

4

Dễ thấy, có 5 giao dịch trên địa chỉ này, họ đã nhận được tổng số 0,09647184 BTC và có số dư cuối cùng là 0,09647184 BTC. Chúng ta có thể thấy rằng họ không sử dụng bất cứ bitcoin nào mà họ nhận được tại địa chỉ đó.

Tiếp tục khám phá giao dịch

Khi bạn quan sát địa chỉ ví Bitcoin, bạn có thể thấy tất cả các giao dịch đã diễn ra trên địa chỉ ví đó.

Trong ví dụ trên có 5 giao dịch, chúng ta có thể tìm hiểu từng giao dịch riêng rẽ, với thông tin về người gửi, người nhận, địa chỉ ví, số tiền gửi và các chi tiết của từng giao dịch.

Tổng kết chương 8

Mỗi địa chỉ cùng với các giao dịch được công khai trên Blockchain Bitcoin. Bạn có thể xem số dư của bất kỳ địa chỉ Bitcoin nào cùng với tất cả các giao dịch của nó. Bên cạnh đó, bạn có thể theo dõi các giao dịch trên Blockchain từ những khối gần nhất cho đến khối đầu tiên – khối được gọi là “Khối Nguyên thủy”.

Hơn nữa, nếu bạn đã thiết lập một ví Bitcoin, bạn có thể sao chép và dán địa chỉ của bạn vào một công cụ khám phá Blockchain Bitcoin và xem thông tin công khai về địa chỉ Bitcoin của bạn. Bạn có thể tham khảo phần nhận bitcoin trong chương này để biết thông tin về cách lấy địa chỉ Bitcoin của bạn.

Nếu bạn đã gửi đi một giao dịch, bạn có thể xem giao dịch đó trên công cụ khám phá Blockchain. Bạn cũng có thể nhấp vào địa chỉ ví nơi bạn gửi giao dịch, và quan sát tất cả các giao dịch khác đã xảy ra trên ví đó.

Trong chương tiếp theo, chúng ta sẽ xem cách thức các khối mới được thêm vào Blockchain như thế nào thông qua quá trình khai thác.

Chương 9Khai thác trong Blockchain

“Công nghệ Blockchain tiếp tục tái định nghĩa không chỉ cách thức địa hạt giao dịch vận hành mà còn nền kinh tế tài chính toàn cầu nói chung.”

- Bob Greifeld, Giám đốc điều hành sàn giao dịch chứng khoán NASDAQ

Bạn có thể đã từng nghe tới cụm từ “khai thác” mà nhiều người sử dụng trong các chủ đề liên quan đến Bitcoin. Trong chương này, chúng ta sẽ tìm hiểu về khái niệm khai thác là gì, cách thức hoạt động ra sao.

Khai thác là gì?

Khai thác là quá trình thêm khối mới vào Blockchain và tạo ra những bitcoin mới. Cứ mỗi khối được thêm vào Blockchain, bitcoin mới sẽ được tạo ra như một phần thưởng cho thợ đào đã thêm được một khối mới vào Blockchain.

Để nhận được phần thưởng cho việc thêm khối mới vào Blockchain cũng giống như khai thác những viên đá quý nhỏ ra khỏi tảng đá lớn. Theo đó, để thu được phần thưởng, chúng ta phải làm rất nhiều công việc, khoan đục một khối đá lớn mới giành được phần thưởng nhỏ cho những nỗ lực bỏ ra.

Thợ đào là một máy tính kết nối với mạng lưới Blockchain của Bitcoin, sẽ thực hiện việc giải quyết một mảnh ghép toán học để thêm khối vào Blockchain. Nếu giải đáp thành công một mảnh ghép toán học, thợ đào hoàn toàn có thể thêm một khối mới vào Blockchain và được tưởng thưởng bằng bitcoin vì nỗ lực đã bỏ ra, đây được gọi là phần thưởng khối.

Mảnh ghép toán học mà thợ đào cố gắng giải quyết rất khó xử lý, nhưng rất dễ xác nhận câu trả lời đúng hay sai một khi nó được tìm thấy. Điều này cũng tương tự như tìm mật mã mở khóa, rất khó đoán, nhưng một khi mật mã khóa được khám phá ra, mọi người đều có thể nhập mã số đó vào để xác thực rằng mật mã đó mở được khóa.

Hoạt động khai thác diễn ra như thế nào?

Khi một giao dịch đã được truyền gửi trên mạng lưới Bitcoin, nó vẫn đang trong quá trình chờ xử lý cho đến khi được thêm vào một khối. Các thợ đào kết nối với mạng lưới Bitcoin có thể chọn bất cứ giao dịch nào đang chờ xử lý để đưa nó vào một khối. Thông thường, họ sẽ chọn các giao dịch có mức phí giao dịch cao nhất để nhận được phí giao dịch cùng với phần thưởng khối.

Một mã băm là dữ liệu xuất của tất cả các giao dịch, một ví dụ về mã băm mà chúng ta đã thấy khi khám phá Blockchain của Bitcoin là:

0000000000000000a2591c88266342e -
6f7380a275d5b98e1882f85347c48db

Một khối chỉ có thể được thêm vào mạng lưới nếu nó có mã băm hợp lệ thấp hơn chỉ tiêu mạng lưới hiện thời. Xử lý mảnh ghép toán học mà các thợ đào đang cố gắng giải đáp chính là tìm ra một số tạo nên một mã băm có giá trị thấp hơn chỉ tiêu mạng lưới.

Việc này tương tự như tung đồng xu hay tung xúc xắc vậy, chỉ tiêu mạng lưới có thể là 4; như thế, nếu bạn tung được số nhỏ hơn 4, bạn có thể thêm một khối hợp lệ vào Blockchain và nhận được phần thưởng khối. Kỹ năng không có vai trò gì trong việc tung được con số thấp hơn, mà chỉ thuần túy là xác suất ngẫu nhiên. Nếu tốc độ tung xúc xắc càng nhanh, bạn càng tung được nhiều lần hơn, và càng có cơ hội tung được con số nhỏ hơn 4.

Mạng lưới Bitcoin được thiết kế để thêm một khối vào Blockchain cứ mỗi 10 phút một lần, và khi nhiều thợ đào tham gia mạng lưới, họ sẽ

tăng cơ hội đoán ra con số nhỏ hơn chỉ tiêu của mạng lưới.

Trong ví dụ về xúc xắc, nếu ai đó cần 10 phút để tung được con số nhỏ hơn 4, thì khi có thêm một người nữa tham gia cùng tung xúc xắc, thì về lý thuyết, thời gian tung được con số nhỏ hơn 4 sẽ giảm đi một nửa. Mạng lưới Bitcoin điều chỉnh bằng cách giảm chỉ tiêu mạng lưới xuống còn 2 để tăng độ khó lên. Bây giờ, họ phải tung được con số nhỏ hơn 2, tức là thấp hơn chỉ tiêu của mạng lưới, và khi đó họ có thể thêm một khối vào Blockchain.

Một khi khối hợp lệ được thêm vào Blockchain, tất cả các thợ đào sẽ lặp lại quá trình này với nhóm các giao dịch tiếp theo để thêm một khối hợp lệ khác vào Blockchain.

Mạng lưới Bitcoin thực hiện việc này trên quy mô lớn hơn, với hàng trăm nghìn máy tính thực hiện việc đoán số ngẫu nhiên để tạo ra mã băm thấp hơn chỉ tiêu của mạng lưới. Và cứ 2.016 khối được thêm vào, chỉ tiêu của mạng lưới sẽ được điều chỉnh để đảm bảo các khối được thêm vẫn 10 phút một lần.

Bằng chứng Xử lý

Quá trình ngẫu nhiên đoán các con số để tạo ra một mã băm hợp lệ và thêm một khối vào Blockchain, được gọi là “Bằng chứng Xử lý”. Quá trình này tiêu tốn rất nhiều điện năng và công suất tính toán, vì thế một mã băm hợp lệ đóng vai trò như một bằng chứng cho thấy công việc đã hoàn thành và các nguồn lực như công suất tính toán cũng như điện năng đã được đóng góp vào mạng lưới.

Công suất tính toán của mạng lưới Bitcoin mạnh hơn 10.000 lần so với 500 siêu máy tính mạnh nhất thế giới kết hợp lại. Với công suất khủng khiếp này, có nhiều người chỉ trích rằng các nguồn lực bị lãng phí vào một quy trình chỉ tạo số ngẫu nhiên.

Những đồng tiền mã hóa khác sử dụng các phương pháp thay thế như Bằng chứng Cổ phần, Bằng chứng Cháy, Bằng chứng Hoạt động và Bằng chứng Dung lượng.

Khai thác và bảo mật

Số lượng thợ đào Bitcoin càng nhiều, mạng lưới càng trở nên an toàn hơn. Bitcoin là một mạng lưới phi tập trung và tất cả các máy tính kết nối trong mạng lưới đều có quyền truy cập Blockchain.

Bất cứ khi nào một giao dịch xảy ra, nó sẽ được cập nhật trên tất cả các máy tính thuộc mạng lưới. Ở đây, bất kỳ máy tính nào cũng đều có thể thêm một khối vào Blockchain, nhưng để việc thêm một khối mới vào Blockchain thành công, thì phần lớn các máy tính trong mạng lưới phải chấp thuận nó là hợp lệ.

Để kiểm soát một mạng lưới phi tập trung, cần phải kiểm soát được hơn 50% công suất tính toán của toàn bộ mạng lưới. Nếu càng có nhiều thợ đào và càng nhiều công suất tính toán được đóng góp vào mạng lưới, thì sẽ càng khó kiểm soát toàn bộ mạng lưới. Do vậy, việc kiểm soát trên 50% máy tính của toàn bộ mạng lưới Bitcoin là một điều gần như bất khả thi.

Hoạt động khai thác có mang lại lợi nhuận không?

Câu trả lời đơn giản là “không”, bởi vì giờ đây, hoạt động khai thác Bitcoin không còn mang lại lợi nhuận trên một máy tính cá nhân nữa.

Độ khó khai thác Bitcoin đã tăng lên, và có nhiều công ty, với khả năng tiếp cận nguồn điện giá rẻ, đã vận hành hàng ngàn máy tính khai thác Bitcoin. Điều này dẫn đến việc khai thác bằng máy tính cá nhân trở nên bất khả thi và vô ích.

Hoạt động khai thác đòi hỏi một lượng điện năng lớn cùng hàng loạt các vi mạch tích hợp chuyên dụng (ASIC). Và ngay cả trong trường hợp nguồn điện được miễn phí, bạn cũng sẽ tốn rất nhiều thời gian mới thu hồi được số vốn phải bỏ ra cho các chi phí mua sắm thiết bị máy tính.

Các vùng khai thác

Nếu sở hữu card đồ họa máy tính khai thác chuyên biệt và khả năng tiếp cận nguồn điện năng giá rẻ hoặc miễn phí, bạn có thể tập hợp công suất tính toán vào một vùng khai thác Bitcoin. Một vùng khai thác kết hợp công suất tính toán của nhiều máy tính nhỏ và tận dụng nguồn lực này để khai thác Bitcoin.

Công việc này đòi hỏi chip máy tính tốc độ cao hoặc chip khai thác chuyên biệt cùng với lượng điện năng khổng lồ; tuy nhiên, các thợ đào với công suất tính toán nhỏ hơn cũng có thể kết hợp công suất tính toán riêng lẻ lại với nhau để cạnh tranh với các khu vực khai thác lớn hơn. Có một loạt các vùng khai thác Bitcoin, và phải nắm vững kiến thức kỹ thuật mới có thể thiết lập dàn máy tính phục vụ cho khai thác, và kết nối nó với một vùng khai thác.

Tám trong 10 vùng khai thác Bitcoin lớn nhất nằm ở Trung Quốc, phần lớn số chúng đều riêng tư và khó gia nhập.

Khai thác trên đám mây

Khai thác trên đám mây là hình thức khai thác mà công suất tính toán được mua lại từ một công ty khai thác lớn, nơi chứa hàng loạt máy tính khai thác chuyên dụng. Các công ty này có thể tiếp cận nguồn điện giá rẻ và sở hữu một lượng lớn các chip máy tính với tốc độ xử lý cao để phục vụ hoạt động khai thác.

Hình thức khai thác trên đám mây tiết kiệm được chi phí đầu tư thiết bị, và giảm bớt hao tổn hằng ngày như điện năng. Chi phí bảo dưỡng cần thành toán thường sẽ được khấu trừ vào bitcoin trước khi trả cho bạn. Hình thức khai thác này còn cung cấp cơ hội khai thác nhiều loại tiền mã hóa đa dạng.

Hình thức khai thác trên đám mây có tiềm năng lớn hơn nhiều so với hình thức khai thác trên máy tính cá nhân có kết nối với một vùng khai thác.

Trong khi phần thưởng khai thác khối có thể khá lớn, hầu hết mọi người không thể tự khai thác thành công một khối được. Họ phải kết hợp công suất tính toán vào một mỏ khai thác hoặc thông qua hình

thức khai thác trên đám mây. Phần thưởng khai thác nhận được thông qua khai thác đám mây và vùng khai thác đối với mỗi người tham gia đóng góp công suất tính toán là rất nhỏ. Mà họ phải tích lũy theo thời gian, tuy nhiên một số ví và sàn giao dịch lại không đồng ý nhận về phần thưởng khai thác, bởi vì điều này sẽ dẫn đến tình trạng có quá nhiều giao dịch quy mô cực kỳ nhỏ cần phải xử lý.

Tổng kết chương 9

Khai thác là quá trình bổ sung các giao dịch vào Blockchain Bitcoin và tạo ra những bitcoin mới.

Thợ đào là những máy tính kết nối với mạng lưới Bitcoin và đóng góp công suất tính toán cũng như các nguồn lực khác vào mạng lưới. Thợ đào sẽ xác minh các giao dịch, tập hợp chúng lại với nhau và tìm ra lời giải cho mảnh ghép toán học, hay còn gọi là “Bằng chứng Xử lý”, đây là minh chứng cho thấy thợ đào đã đóng góp công suất tính toán và nguồn lực vào mạng lưới Bitcoin.

Các giao dịch được nhóm lại với nhau trong một khối. Một khi thợ đào đã tập hợp được các giao dịch lại với nhau và giải quyết thành công thuật toán Bằng chứng Xử lý, thợ đào hoàn toàn có thể thêm một khối hợp lệ các giao dịch vào Blockchain. Mỗi khối được thêm vào đều liên kết với các khối trước đó để tạo thành một chuỗi các khối. Độ khó của thuật toán Bằng chứng Xử lý được điều chỉnh sau mỗi 2.016 khối để đảm bảo rằng các khối được liên tục thêm vào Blockchain khoảng 10 phút một lần.

Thợ đào được tưởng thưởng bằng các khoản phí giao dịch và phần thưởng khối cho mỗi khối giao dịch hợp lệ mà họ thêm được vào Blockchain của Bitcoin. Những phần thưởng này được thiết lập theo cơ chế giảm dần qua thời gian, và đến cuối cùng, thợ đào chỉ còn nhận được các khoản phí trên các giao dịch đi kèm theo khối mà họ thêm được vào Blockchain.

Hầu hết các khối đã được khai thác tại những vùng khai thác lớn hoặc từ các nhóm thợ đào tập hợp công suất tính toán của họ lại với nhau. Việc khai thác tiêu tốn rất nhiều công suất tính toán cũng

như điện năng, nên hiện nay không còn hiệu quả và khả thi trên quy mô nhỏ nữa.

Hình thức khai thác trên đám mây là cách khai thác sử dụng công suất tính toán mua lại từ một công ty khai thác lớn, nơi sở hữu một dàn máy tính khai thác chuyên dụng. Công suất tính toán đó được đóng góp vào một vùng khai thác, rồi kết hợp với công suất tính toán của nhiều máy tính khác để cùng khai thác khối. Phần thưởng khối mới này sau đó sẽ được các thợ đào tham gia khai thác chia sẻ với nhau.

Không chỉ các khối của Bitcoin mà của nhiều đồng tiền mã hóa khác cũng có thể khai thác được. Nhiều trong số chúng sử dụng các thuật toán khác nhau đòi hỏi công suất tính toán ít hơn và lượng điện năng tiêu thụ nhỏ hơn, khi so sánh với thuật toán Bằng chứng Xử lý của Bitcoin.

Trong chương tiếp theo, chúng ta sẽ tìm hiểu về một số thuật toán được sử dụng trong các đồng tiền mã hóa nổi tiếng khác và so sánh chúng với thuật toán của Bitcoin.

Chương 10Ethereum, Bitcoin Cash và các loại tiền mã hóa khác

“Khi nảy ra kế hoạch về Ethereum, ý nghĩ đầu tiên của tôi là thứ này tuyệt vời quá đến mức khó mà thành hiện thực. Nhưng hóa ra, ý tưởng cốt lõi của Ethereum về cơ bản là tốt và hoàn toàn hợp lý.”

- Vitalik Buterin, nhà sáng lập Ethereum

Nếu từng tìm hiểu về Bitcoin và tiền ảo, có thể bạn đã biết tới Ethereum, Litecoin, Ripple và nhiều đồng tiền mã hóa khác.

Từ Altcoin được sử dụng để chỉ những loại tiền mã hóa tương tự như Bitcoin. Altcoin là viết tắt của “Alternative Coins” (những đồng tiền thay thế) hoặc “Alternative Bitcoin” (Bitcoin thay thế).

Trong chương này, chúng ta sẽ tìm hiểu một vài đồng tiền mã hóa nổi tiếng khác và sự khác biệt của chúng với Bitcoin.

Ethereum

Ethereum là đồng tiền mã hóa có giá vốn hóa thị trường lớn thứ hai sau Bitcoin. Nhiều người dự đoán Ethereum sẽ vượt Bitcoin để trở thành đồng tiền mã hóa lớn nhất trong tương lai.

Trong khi mạng lưới Bitcoin được sử dụng chủ yếu cho các giao dịch tài chính và hoạt động thanh toán, mạng lưới Ethereum cho phép mọi người xây dựng các ứng dụng phi tập trung (dApp) và các hợp đồng thông minh chạy trên Blockchain.

Lưu ý: Ứng dụng phi tập trung (dApp) và hợp đồng thông minh sẽ được đề cập chi tiết hơn trong phần tiếp theo.

Blockchain là một trong những công nghệ nền tảng trọng yếu của Bitcoin, tuy nhiên Bitcoin chỉ là một ví dụ về khả năng ứng dụng của công nghệ Blockchain. Trong khi đó, Ethereum được coi là đồng tiền mã hóa sẽ giúp chúng ta tìm hiểu và đa dạng hóa các khả năng của công nghệ Blockchain hơn so với Bitcoin.

Như đã đề cập, mạng lưới Bitcoin mạnh hơn 500 siêu máy tính lớn nhất thế giới gộp lại. Tuy nhiên, hầu hết công suất xử lý của mạng lưới Bitcoin đều bị xem là lãng phí vì chỉ tập trung đóng góp cho quá trình tạo số ngẫu nhiên trong thuật toán Bằng chứng Xử lý để thêm các khối vào Blockchain.

Trong khi đó, mạng lưới Ethereum cho phép lập trình viên và các công ty tạo ra các ứng dụng chạy trên một mạng lưới máy tính phi tập trung. Điều này sẽ tận dụng công suất tính toán của mạng lưới tốt hơn, và giúp các ứng dụng vận hành trên toàn mạng lưới, chứ không chỉ trên một máy chủ trung tâm.

Ứng dụng phi tập trung

Hiện nay, hầu hết các ứng dụng và các trang web đều theo mô hình tập trung, tức là chúng được cài đặt và vận hành từ một máy chủ trung tâm.

Ví dụ, khi bạn đăng tải ảnh lên Facebook, bức ảnh đó sẽ được lưu trữ trên các máy chủ của Facebook. Facebook kiểm soát tất cả các máy chủ và dữ liệu trong đó. Nếu máy chủ của Facebook bị trục trặc dẫn đến ngừng hoạt động hoặc bị tấn công, toàn bộ hình ảnh và thông tin trên đó sẽ trục trặc theo.

Đối với những người sống ở các quốc gia nơi chịu sự điều hành của chế độ độc tài, các chính phủ có thể ra lệnh đóng vĩnh viễn các máy chủ và các trang web theo mô hình tập trung có chứa bất cứ thông tin quan trọng nào của chính phủ.

Các ứng dụng phi tập trung sử dụng công suất tính toán, không gian lưu trữ và tài nguyên của toàn bộ mạng lưới máy tính kết nối với nó.

Chúng không chịu sự kiểm soát của một thực thể duy nhất nào và cũng không vận hành trên các máy chủ tập trung.

Các ứng dụng phi tập trung chạy trên tất cả các máy tính kết nối với mạng lưới. Khi các bức ảnh được tải lên, chúng được phân phối khắp mạng lưới, nên dù một trong số các máy tính đó bị tấn công hoặc gặp trục trặc dẫn đến ngừng hoạt động, thì các máy tính khác sẽ không bị ảnh hưởng gì.

Các chính phủ không thể đóng cửa các trang web hoặc máy chủ mà họ phản đối, bởi vì dù có loại bỏ một máy tính ra khỏi mạng lưới, thì ứng dụng và thông tin vẫn sẽ được vận hành khắp các máy tính còn lại của mạng lưới.

Hợp đồng thông minh

Hợp đồng thông minh là những hợp đồng cho phép thực thi các thỏa thuận đã được quy định từ trước mà không cần sự có mặt của bên thứ ba như luật sư hay tòa án. Chúng được viết bằng một ngôn ngữ lập trình máy tính chạy trên Blockchain. Mã máy tính sẽ tự động xác minh hợp đồng, thực thi và thúc ép thực hiện các điều khoản hợp đồng. Mức độ tự quản của các hợp đồng thông minh có thể được quy định trước, vì chúng có thể tự thực thi và tự ép buộc thực hiện một phần hoặc toàn phần thỏa thuận trong hợp đồng.

Hợp đồng thông minh không phải là các giao dịch tài chính đơn thuần, vì gần như mọi giá trị đều có thể được trao đổi thông qua việc sử dụng hợp đồng thông minh. Các công ty hiện đang thiết lập các hợp đồng thông minh trong nhiều ngành công nghiệp khác nhau như bản quyền âm nhạc, chương trình khách hàng trung thành, chương trình bảo hành sản phẩm, ảnh kỹ thuật số tự xác thực, hợp đồng bảo hiểm, v.v...

Những lợi ích của hợp đồng thông minh

Một rủi ro lớn đối trong các giao dịch Bitcoin là nếu bạn gửi bitcoin đến một địa chỉ nào đó, thì người nhận tự động có toàn quyền sở hữu số bitcoin kia. Nói cách khác, một khi giao dịch đã hoàn tất,

không có cách nào để đảo chiều giao dịch, yêu cầu hoàn tiền hay liên hệ với bên trung gian nào nếu xảy ra tranh chấp hoặc có vấn đề phát sinh với giao dịch.

Nếu bạn đang mua hàng và thanh toán trước khi nhận hàng bằng cách gửi bitcoin đến địa chỉ của người bán, thì sẽ không có gì đảm bảo rằng người bán sẽ gửi hàng cho bạn. Ví Bitcoin còn có đặc tính ẩn danh, nên bạn sẽ không có cách nào liên hệ với người mà bạn đã gửi bitcoin đó. Trong trường hợp bitcoin bị gửi đến nhầm địa chỉ hoặc người bán không chuyển cho bạn các mặt hàng như trong thỏa thuận mua bán, thì số bitcoin ấy của bạn bị coi là đã mất và bạn không có cách nào lấy lại nữa.

Hợp đồng thông minh có thể giảm thiểu nhiều rủi ro liên quan đến giao dịch, vì chúng hoạt động tương tự như một tổ chức trung gian nhằm đảm bảo các thỏa thuận trong giao dịch được đáp ứng và thực thi.

Thẻ Ethereum và các chương trình ICO

Ethereum cho phép lập trình viên tạo ra đồng tiền riêng của họ trên Blockchain của Ethereum, hay còn gọi là thẻ (token). Điều này cho phép các công ty nhanh chóng tận dụng được công nghệ Blockchain mà không cần phải khởi tạo và quản lý Blockchain riêng của họ.

Gần đây, có rất nhiều tổ chức huy động vốn thông qua các đợt ICO, trong đó thường là các thẻ được phát hành trên mạng lưới Ethereum. Nhiều đồng tiền mới này được tạo ra không phải những đồng tiền mã hóa độc lập với Blockchain riêng của chúng, mà là các thẻ được phát hành trên Blockchain của Ethereum.

Ethereum và Blockchain 2.0

Như đã đề cập, một trong những công nghệ nền tảng chính của Bitcoin là công nghệ Blockchain. Bitcoin tạo ra Blockchain đầu tiên, đây được coi là Blockchain 1.0, và được sử dụng chủ yếu như sổ cái phân tán để lưu trữ các giao dịch trên mạng lưới Bitcoin.

Ethereum đưa tiềm năng của Blockchain vượt xa ý tưởng ban đầu của nó. Những triển vọng mà nền tảng Ethereum hiện thực hóa các ứng dụng phi tập trung và hợp đồng thông minh, có thể được coi như Blockchain 2.0.

Khi thảo luận về tương lai của công nghệ Blockchain, người ta thường đề cập đến Blockchain 2.0, các ứng dụng phi tập trung và hợp đồng thông minh. Tiềm năng mới của Blockchain 2.0 được dự đoán sẽ có tác động tới thế giới mạnh mẽ hơn nhiều so với Bitcoin. Blockchain 2.0 đưa công nghệ Blockchain vào các lĩnh vực vượt ra ngoài phạm vi các giao dịch tài chính.

Sự khác biệt giữa Ethereum và Bitcoin

Bitcoin là một sổ cái phân tán phi tập trung chủ yếu được sử dụng cho các giao dịch tài chính, nhưng Ethereum là một nền tảng điện toán phi tập trung chủ yếu được sử dụng để vận hành các ứng dụng và các hợp đồng thông minh.

Bitcoin được thiết kế để dùng thanh toán và trao đổi giá trị. Đồng tiền trên mạng lưới Ethereum có tên “Ether” được thiết kế sử dụng như một khoản chi trả cho công suất tính toán khi chạy các ứng dụng phi tập trung và hợp đồng thông minh.

Ethereum cùng với đồng tiền Ether không hề được thiết kế để thay thế Bitcoin. Nó phục vụ một mục đích hoàn toàn khác. Và mặc dù nó ngày càng trở nên phổ biến và tăng giá trị nhanh hơn so với Bitcoin, nó không phải đối thủ cạnh tranh với Bitcoin trong các giao dịch tài chính.

Litecoin

Litecoin được xây dựng trên cùng một nền tảng với Bitcoin, nhưng nó tách ra từ Blockchain Bitcoin nguyên thủy để trở thành một Blockchain cũng như một loại tiền mã hóa hoàn toàn khác.

Mạng lưới Bitcoin là mạng lưới tiền mã hóa lớn nhất, và đa số thành viên trong mạng lưới thường phải đồng thuận về hướng phát triển

của mạng lưới hay những thay đổi cho mã lập trình. Vì mạng lưới Bitcoin quá lớn, nên toàn mạng lưới đã bị trì trệ trong nhiều năm vì không thể đạt được sự đồng thuận trong nhiều quyết định thay đổi.

Litecoin có thể đạt được nhiều cải thiện đáng kể trong mạng lưới so với Bitcoin. Litecoin thêm một khối vào Blockchain cứ mỗi 2,5 phút một lần, trong khi đó, với Bitcoin là cứ 10 phút một lần. Trên mạng lưới Litecoin, kích thước khối cũng nhỏ hơn, đồng nghĩa với nhiều giao dịch hơn được bao gồm trong mỗi khối.

Litecoin xử lý giao dịch cũng như các khoản thanh toán nhanh hơn và tiếp tục thực hiện nhiều cải tiến trong khi mạng lưới Bitcoin vẫn vật vã để đạt được sự đồng thuận của đa số thành viên cho nhiều đề xuất thay đổi.

Một số người tin rằng, trong tương lai, Litecoin sẽ là mạng lưới thanh toán và giao dịch tốt hơn, được sử dụng rộng rãi hơn Bitcoin.

Ripple

Ripple là một mạng lưới thanh toán tiền mã hóa đang được tạo nên thông qua quá trình hợp tác với các tổ chức tài chính lớn. Nó được dự báo là sẽ trở thành mạng thanh toán toàn cầu mới để giải quyết các giao dịch giữa các ngân hàng và các tổ chức tài chính.

Bitcoin cùng với công nghệ Blockchain nền tảng của nó được nhìn nhận như một cách thức loại bỏ cơ chế quản lý thanh toán tập trung của các chính phủ, ngân hàng và tổ chức tài chính.

Bitcoin và công nghệ Blockchain nguyên thủy được thiết lập với một mã nguồn mở và phi tập trung. Với những đặc điểm này, mỗi người trên mạng lưới đều có thể xem xét mã Bitcoin và giao dịch trực tiếp với nhau mà không cần đến các tổ chức trung gian tài chính.

Ripple không mang đặc tính phi tập trung hay mã nguồn mở, mà các ngân hàng và tổ chức tài chính lớn ứng dụng công nghệ Blockchain mã nguồn mở và phi tập trung và biến nó trở thành các hệ thống mã nguồn đóng, tập trung, truyền thống.

Dù Ripple có thể thay đổi cách thức các ngân hàng và các tổ chức tài chính xử lý giao dịch, thì đối với nhiều người, nó đi ngược với mục đích ban đầu mà Bitcoin và công nghệ Blockchain được tạo ra và hướng đến vì nó lại đặt quyền lực và khả năng kiểm soát thanh toán vào tay các tổ chức tài chính lớn.

Bitcoin Cash

Trên Blockchain Bitcoin, có một số hữu hạn các giao dịch có thể được bao gồm trong mỗi khối. Một khối là một tập dữ liệu giao dịch, kích thước tập tin được giới hạn trong 1MB. Mỗi giao dịch được thêm vào sẽ tăng kích thước tập tin, và một khi kích thước tập dữ liệu đạt đến 1MB, không thể giao dịch nào vào khối đó nữa.

Một khối sẽ được thêm vào Blockchain cứ 10 phút một lần, vì vậy bất kỳ giao dịch nào đang trong quá trình chờ mà chưa được thêm vào một khối đều phải chờ tối thiểu 10 phút mới được xử lý. Theo đó, càng nhiều giao dịch diễn ra trên Blockchain Bitcoin, thì càng nhiều giao dịch kẹt trong quá trình chờ xử lý. Điều này dẫn đến tình trạng tồn đọng các giao dịch chưa được xử lý và thời gian xử lý giao dịch sẽ trở nên chậm hơn.

Bitcoin Cash được tạo ra khi mạng lưới Bitcoin không thể đạt được sự đồng thuận về việc thay đổi nào sẽ được thực thi để giải quyết những vấn đề này. Sự bất đồng này dẫn đến một phần trong mạng chia tách ra để tạo nên loại tiền mã hóa lấy tên Bitcoin Cash.

Bitcoin Cash được tạo ra nhằm giải quyết vấn đề về thời gian xử lý chậm bằng cách gia tăng đáng kể kích thước tập tin. Nó cho phép một số lượng gần như vô hạn các giao dịch trong mỗi khối. Bên cạnh đó, còn nhiều tính năng khác mà các nhà phát triển Bitcoin Cash dự kiến sẽ thực hiện để cải thiện chức năng của Bitcoin Cash khi so sánh với Bitcoin.

Sự khác nhau giữa Bitcoin và Bitcoin Cash

Mặc dù trong tên Bitcoin Cas h có chứa từ “Bitcoin”, nhưng nó không phải Bitcoin. Chỉ có duy nhất một Bitcoin, với tên “Bitcoin”, và

không có thêm từ nào khác. Nó là Blockchain Bitcoin nguyên thủy được tạo ra, mà sau này, hầu hết các tiền mã hóa thay thế đều dựa vào đó.

Bitcoin Cash là một Altcoin, nó sao chép Blockchain và mã nguồn của Bitcoin để tạo ra đồng tiền mã hóa mới. Tất cả những người giữ tiền Bitcoin tại thời điểm chia tách đều có quyền nhận khoản Bitcoin Cash tương ứng.

Rất dễ tạo ra một đồng tiền mã hóa mới, và có hàng ngàn đồng tiền mã hóa khác tương tự như Bitcoin Cash. Hầu hết chúng cũng sao chép Blockchain và mã nguồn của Bitcoin trước khi tạo ra đồng tiền mã hóa của riêng chúng. Trong số đó có nhiều loại tiền mã hóa cũng có từ "Bitcoin" trong tên, chẳng hạn như Bitcoin Dark và Bitcoin Plus.

Mua Bitcoin Cash cũng tương tự như mua Bitcoin Dark, Bitcoin Plus hay Litecoin. Tất cả đều là những đồng tiền mã hóa thay thế có thể sử dụng tương tự Bitcoin. Tuy nhiên, chúng không phải Bitcoin, và không có mấy khả năng được chấp nhận như một phương thức thanh toán hay cất trữ giá trị trong tương lai.

Bitcoin Cash mới được tạo ra và chưa thực hiện được nhiều đề xuất thay đổi đã được tạo ra trước đó. Hiện vẫn chưa rõ những lợi ích và tính năng nào của Bitcoin Cash có thể coi là vượt trội hơn so với Bitcoin.

Tổng kết chương 10

Chương này đề cập đến chỉ một số ít ỏi trong hàng ngàn loại tiền mã hóa hiện nay, và có nhiều đồng tiền mã hóa khác đang được tạo ra mỗi ngày. Trang web Coin Market Cap có bản danh sách cập nhật đầy đủ các đồng tiền mã hóa hiện hành kèm thông tin chi tiết như mức giá, giá trị vốn hóa thị trường cùng nhiều thông tin khác.

Chương 11Ảnh hưởng và tương lai của Bitcoin

“Bitcoin, và ý tưởng đằng sau nó, sẽ là bước đột phá đối với các quan niệm tiền tệ truyền thống.

Kết quả, tiền tệ sẽ tốt hơn nhờ nó.”

- Edmund Moy, giám đốc thứ 38 của Cục Đúc tiền Kim loại Hoa Kỳ, ngày 23 tháng 05 năm 2014

Ảnh hưởng hiện tại của Bitcoin

Mặc dù Bitcoin hiện không phải phương thức thanh toán phổ biến, nhưng nó tạo nên ảnh hưởng to lớn bằng cách tuyên cáo cho thế giới biết rằng tiền tệ có thể tồn tại ngoài sự kiểm soát của ngân hàng và chính phủ.

Tác động này không thể xem nhẹ, khi mọi người luôn chịu sự kiểm soát của chính phủ và hệ thống tài chính nơi họ sinh ra.

Việc thế giới liên tục hướng tới viễn cảnh số hóa toàn diện đã giúp hoạt động giám sát và theo dõi người dân trở nên dễ dàng hơn đối với các chính phủ. Chỉ trong tháng này, Trung Quốc đã bắt đầu cấm người dân sử dụng nhiều tính năng trong chương trình WhatsApp, một trong những ứng dụng trò chuyện phổ biến nhất thế giới, vì chương trình này không chấp nhận chia sẻ thông tin cá nhân người dùng với chính phủ.

Chính phủ kiểm soát tiền tệ và các hệ thống tài chính thậm chí còn bị kiểm soát chặt chẽ hơn, rồi đến Internet. Các chính phủ có thể tịch thu tài khoản ngân hàng và giới hạn hoạt động thanh toán đối với tổ chức, mà WikiLeaks là ví dụ điển hình. Tất cả các khoản thanh toán điện tử đều có thể được chính phủ theo dõi dễ dàng, từ đó chính phủ có nhiều khả năng buộc tội nhiều người nếu họ tham

gia giao dịch hoặc ủng hộ cho các tổ chức hay cá nhân mà chính phủ không cho phép.

Chính phủ cũng kiểm soát nguồn cung tiền, như trong trường hợp của Zimbabwe, điều này đã dẫn đến sự mất giá hoàn toàn của đồng nội tệ. Ngân hàng trung ương cũng có thể in thêm tiền hoặc điều chỉnh lãi suất, từ đó ảnh hưởng trực tiếp đến giá trị đồng tiền. Người dân ở các nước như Zimbabwe có thể thấy thu nhập và tiền tiết kiệm của họ trở nên vô giá trị do khả năng quản lý tiền tệ yếu kém của chính phủ.

Con người còn hoạt động trong nhiều nền kinh tế riêng lẻ, mà nhiều người trong số đó bị tách ra khỏi phần còn lại của thế giới. Để kinh doanh trên phạm vi quốc tế, bạn phải mở nhiều tài khoản ngân hàng chuyên dụng với các tổ chức tài chính và chấp nhận những khoản phí giao dịch quốc tế đắt đỏ. Còn nhiều người trên thế giới không thể tiếp cận các tài khoản ngân hàng hay tổ chức tài chính, mà thiếu đi sự trợ giúp của những tổ chức này, họ không thể giao dịch với phần còn lại của thế giới. Ngay cả với những người gửi tiền cho gia đình, bạn bè hoặc các doanh nghiệp ở các nước khác, việc hoàn thiện giao dịch cũng phải mất một khoảng thời gian dài, kéo theo nhiều chi phí đáng kể phát sinh thông qua phí giao dịch cao và những mức tỷ giá hối đoái bất lợi.

Bitcoin cho phép tiền tồn tại ngoài sự kiểm soát của chính phủ. Hơn nữa, nguồn cung bitcoin là một con số cố định, nên nó sẽ không thể mất giá vì dư thừa bitcoin. Điều này không có nghĩa là giá trị của Bitcoin sẽ tăng lên, vì điều này phụ thuộc vào việc mọi người có chấp nhận nó như một hình thức thanh toán hay không. Tuy nhiên, với Bitcoin, các chính phủ không thể kiểm soát giá trị thông qua hành động in thêm tiền hay thay đổi mức lãi suất. Mà giá trị được xác định bởi các lực lượng cung và cầu trên thị trường tự do, cùng với sự chấp nhận nó như một hình thức thanh toán đúng nghĩa của công chúng.

Ví Bitcoin có thể được thiết lập dưới chế độ ẩn danh, theo đó, trong trường hợp chiếc ví được thiết lập hợp lệ, chính phủ không thể liên kết ví ẩn danh đó tới nhiều người được. Chính phủ cũng không thể

tịch thu ví Bitcoin ẩn danh hoặc hạn chế hoạt động thanh toán. Và những người sống trong chế độ độc tài có thể tạo ra các nhóm mà tại đó, họ có thể nhận tiền tài trợ và thực hiện giao dịch, mà không cần chịu sự kiểm soát thanh toán của chính phủ.

Mọi người trên khắp thế giới có thể thực hiện các giao dịch quốc tế dễ dàng như gửi email. Ví Bitcoin có thể được thiết lập trong vòng vài phút mà không cần phải thực hiện thủ tục xác minh dài dòng, và bitcoin có thể được gửi và nhận từ bất cứ đâu trên thế giới, ngay sau khi thiết lập ví thành công. Điều này cho phép mọi người trên khắp thế giới trở thành một bộ phận trong hệ thống tài chính toàn cầu, cũng như một bộ phận của thị trường mà trước đây họ đã bị loại trừ ra khỏi.

Bitcoin đã tạo ra tiềm năng trong đó tiền tệ, các giao dịch, các tài khoản ngân hàng và toàn bộ nền kinh tế có thể tồn tại ngoài sự kiểm soát của chính phủ và các hệ thống tài chính hiện thời. Điều này tác động tới quan niệm về cách vận hành của tiền tệ và thị trường tài chính, và mang đậm tính cách mạng hóa.

Hiện Bitcoin vẫn còn đang trong giai đoạn trứng nước, và ảnh hưởng tiềm tàng của Bitcoin có thể lớn hơn rất nhiều lần so với những gì mà nó đã tạo nên. Các chính phủ, tổ chức và công ty mới chỉ bắt đầu nhận ra tiềm năng ứng dụng của Bitcoin cũng như của các công nghệ nền tảng đằng sau Bitcoin.

Trong phần tiếp theo, chúng ta sẽ thảo luận về tiềm năng và các vấn đề phát sinh trong tương lai có thể ảnh hưởng đến Bitcoin.

Tương lai của Bitcoin

Vấn đề về khả năng mở rộng

Như đã đề cập, Bitcoin có năng lực xử lý khoảng 6 giao dịch một giây, trong khi đó mạng thanh toán Visa là hơn 20.000 giao dịch mỗi giây. Bitcoin phải có khả năng xử lý nhiều giao dịch trong khoảng thời gian ngắn hơn mới có thể hy vọng thay thế được các phương thức thanh toán hiện tại.

Hiện tại, Bitcoin có nhiều hạn chế về tốc độ giao dịch, nên viễn cảnh Bitcoin trở thành mạng lưới thanh toán quy mô lớn khó mà thành hiện thực. Đây là một vấn đề nghiêm trọng đối với Bitcoin trong vài năm qua, khi mà mạng lưới và cộng đồng bị chia tách về cách thức giải quyết vấn đề này.

Gần đây, một phần mạng lưới đã tách ra để tự tạo tiền mã hóa riêng của họ. Điều này có nghĩa là, mạng lưới Bitcoin cuối cùng đã đi đến sự nhất trí chung về cách thức giải quyết các vấn đề về khả năng mở rộng.

Mạng Bitcoin Unlimited, SegWit và Lightning

Các vấn đề về khả năng mở rộng liên quan tới số lượng giao dịch có thể được bao gồm trong khối và tần suất các khối được thêm vào Blockchain. Hiện tại, kích thước khối Bitcoin là 1MB và một khối được thêm vào Blockchain cứ 10 phút một lần. Khi kích thước dữ liệu của các giao dịch trong khối đạt đến 1MB, sẽ không thể thêm vào khối bất cứ giao dịch nào nữa và các giao dịch đang chờ xử lý sẽ phải đợi cho đến khối tiếp theo.

Bitcoin Unlimited là một đề xuất để giải quyết các vấn đề về khả năng mở rộng. Đa số thành viên mạng lưới không tán thành giải pháp này, nên một phần ủng hộ đã tách ra và tự tạo cho mình một đồng tiền mã hóa mới với tên “Bitcoin Cash”. Họ sẽ thực hiện giải pháp này trong Bitcoin Cash, chi tiết sẽ được đề cập đến trong phần tiếp theo của cuốn sách.

SegWit, hay Nhân chứng Tách rời, là một đề xuất khác để sửa chữa vấn đề về khả năng mở rộng. Cụ thể, đề xuất này vẫn giữ nguyên kích thước khối hiện tại ở mức 1MB, nhưng sẽ tách riêng chữ ký trên một giao dịch sao cho nó không còn được bao gồm trong một khối.

Chữ ký là một yêu cầu dùng để xác nhận việc người gửi có quyền truy cập một địa chỉ và được phép thực hiện hoạt động truyền gửi giao dịch. Một khi chữ ký được xác nhận là hợp lệ, nó sẽ không còn cần thiết nữa. Việc tách chữ ký khỏi dữ liệu giao dịch sẽ cho phép

nhiều giao dịch được xử lý trong thời gian ngắn hơn trong khi vẫn đảm bảo giới hạn kích thước khối là 1MB.

SegWit gần đây đã nhận được sự đồng thuận của mạng lưới Bitcoin, và sẽ được triển khai trong tương lai gần. Khi SegWit được triển khai, nó sẽ cho phép Bitcoin thực thi giải pháp "Mạng Lightning".

Mạng Lightning sẽ gia tăng đáng kể số lượng giao dịch có thể được xử lý, với ước tính hàng triệu giao dịch mỗi giây. Mạng Lightning còn sử dụng các hợp đồng thông minh được xử lý bên Blockchain. Điều này đồng nghĩa với việc các giao dịch riêng lẻ được xử lý ngay lập tức vì chúng không cần đợi để được thêm vào một khối trên Blockchain Bitcoin trước khi chúng được xử lý.

Đồng thời, phí giao dịch sẽ giảm xuống, và mạng Lightning sẽ cho phép xử lý các khoản thanh toán vi mô với những khoản bitcoin rất nhỏ. Ngoài ra, mạng Lightning cũng cho phép quá trình trao đổi tức thì giữa Bitcoin với nhiều loại tiền mã hóa khác có hỗ trợ công nghệ này.

Nếu mạng Lightning được triển khai và có khả năng thực hiện những gì nó tuyên bố, thì tương lai của Bitcoin sẽ tràn đầy hứa hẹn.

Bitcoin Cash và hai loại Bitcoin phái sinh

Toàn mạng lưới Bitcoin không thể đạt được sự đồng thuận về hướng phát triển trong tương lai nên một phần trong mạng lưới đã tách ra để tạo nên đồng tiền Bitcoin Cash.

Bitcoin Cash là một bản sao của mã nguồn Bitcoin nguyên thủy, nhưng Bitcoin và Bitcoin Cash là hai loại tiền mã hóa hoàn toàn khác nhau. Những thành viên ủng hộ Bitcoin Cash có kế hoạch tăng tốc độ quá trình xử lý giao dịch và cải thiện nhiều chức năng mà họ không thể thực hiện với Bitcoin.

Như đã đề cập, khả năng xử lý giao dịch của mạng lưới Bitcoin bị hạn chế bởi giới hạn kích thước khối là 1MB và khung thời gian xử

lý 10 phút. Điều này đã dẫn đến tình trạng tồn đọng giao dịch trên mạng lưới Bitcoin, và ngăn không cho Bitcoin được sử dụng trên một quy mô lớn hơn.

Một trong những đề xuất để giải quyết các vấn đề về khả năng mở rộng là Bitcoin Unlimited, trong đó nó cho phép Bitcoin Cash đưa vô số giao dịch vào mỗi khối. Bitcoin Unlimited đã bị đa số các thành viên trên mạng lưới Bitcoin bác bỏ, và đó là lý do tại sao một phần của mạng lưới đã tách ra để thực hiện việc nâng cấp kích thước khối và nhiều tính năng khác.

Nhiều người lo ngại rằng sẽ có sự nhầm lẫn

đâu là Bitcoin thực được chấp nhận cho các giao dịch. Và nếu điều này xảy ra, nó có thể làm chậm quá trình giành lấy sự chấp thuận từ công chúng của Bitcoin.

Như đã được đề cập trong chương về lịch sử tiền tệ, giá trị của đồng tiền chủ yếu dựa vào việc mọi người có chấp nhận nó như một hình thức thanh toán hay không. Do đó, mọi người có chấp nhận Bitcoin Cash hay các giải pháp thay thế Bitcoin khác trong tương lai hay không còn rất mơ hồ.

Còn quá sớm để khẳng định tương lai của Bitcoin Cash, khi mà nó có thể trở thành một phương án thay thế khả thi hoặc trở nên vô giá trị như hàng ngàn đồng tiền mã hóa khác đã được tạo ra.

Bitcoin và cơ hội trở thành một giải pháp thanh toán thay thế chính thống

Bitcoin hiện đang được chấp nhận tại nhiều cửa hàng trên toàn thế giới, tuy nhiên phạm vi chấp nhận và sử dụng này vẫn chỉ dừng ở quy mô nhỏ. Bạn có thể thanh toán bằng bitcoin tại quán cà phê ở San Francisco, nhưng lại không thể làm như vậy tại các quán cà phê Starbucks trên toàn thế giới.

Apple Pay, Samsung Pay và PayPal đang trở thành những giải pháp thanh toán thay thế được nhiều người sử dụng song song với thẻ

tín dụng và tiền mặt. Bitcoin còn cả một chặng đường dài để đi trước khi có thể trở thành giải pháp thanh toán chính thống cùng với các lựa chọn hiện có. Các doanh nghiệp có chấp nhận Bitcoin như một phương thức thanh toán hay không tùy thuộc vào nhu cầu của khách hàng. Nếu có nhiều người sử dụng Bitcoin, chủ doanh nghiệp có thể sẽ quan tâm và chấp nhận nó như một phương thức thanh toán tại cửa hàng của họ.

Hiện nay, nhu cầu tiêu dùng Bitcoin thường nằm ở khu vực biên giới, trong khi đó người tiêu dùng am hiểu về công nghệ thích ý tưởng sử dụng Bitcoin trong cửa hàng. Không có khả năng doanh nghiệp sẽ mất khách hàng chỉ vì không chấp nhận Bitcoin như một phương thức thanh toán. Số lượng khách hàng nhận được lợi ích khi sử dụng Bitcoin như phương thức thanh toán vẫn còn ở mức tối thiểu, và với họ phương thức thanh toán mới này còn quá lạ lẫm so với một giải pháp thanh toán hữu hiệu như PayPal.

Khi ngày càng nhiều người sử dụng Bitcoin, càng nhiều khả năng doanh nghiệp coi nó như một phương thức thanh toán hơn. Việc chấp nhận Bitcoin như một giải pháp thanh toán thay thế sẽ gắn liền với việc người tiêu dùng có thừa nhận đồng tiền Bitcoin hay không. Một khi ngày càng nhiều khách hàng tiềm năng sử dụng Bitcoin, sẽ ngày càng nhiều doanh nghiệp chấp nhận nó, từ đó dẫn đến kỳ vọng của người tiêu dùng rằng, khi họ tham gia hoạt động kinh doanh nào đó, doanh nghiệp đó sẽ chấp nhận Bitcoin.

Bitcoin và cơ hội trở thành đồng tiền quốc tế trong tương lai

Ngay bây giờ, thật khó mà hình dung nổi viễn cảnh này, tuy nhiên, nói Bitcoin có tiềm năng trở thành đồng tiền quốc tế trong tương lai cũng không quá lời.

Khi chúng ta suy nghĩ tới các loại tiền tệ quốc tế, thì đồng đô la Mỹ là loại tiền tệ chính mà chúng ta nhớ đến, nó được sử dụng để làm đồng tiền chủ yếu ở nhiều quốc gia. Tại bất cứ nơi nào trên thế giới mà bạn đến, đồng đô la Mỹ đều sẽ là loại tiền tệ chính được chấp nhận để sang đồng nội tệ ở đó. Không có khả năng xuất hiện một

doanh nghiệp đổi tiền tuyên bố không chấp nhận đồng đô la Mỹ mà lại chấp nhận một loại tiền tệ nhỏ như Việt Nam đồng.

Đồng euro có thể được coi như một đồng tiền quốc tế. Bạn có thể nhận lương bằng đồng euro ở nước này rồi chi tiêu tại hàng loạt các quốc gia khác chấp nhận nó. Các ngôn ngữ và các nền văn hóa ở mỗi quốc gia đều khác nhau, nhưng tất cả đều sử dụng cùng một loại tiền tệ.

Viễn cảnh mọi quốc gia đều chấp nhận Bitcoin như đồng tiền chính là một điều có vẻ không tưởng. Tuy nhiên, trong tương lai, Bitcoin có thể được thừa nhận rộng rãi với tư cách một đồng tiền quốc tế. Hiện nay, đã có một số các doanh nghiệp chấp nhận thanh toán bằng đồng tiền địa phương hoặc bằng bitcoin. Khi Bitcoin dần được mọi người đón nhận trên khắp thế giới, nhiều cửa hàng ở các quốc gia có thể chấp nhận nó với vai trò phương thức thanh toán.

Mặc dù bạn có thể mang theo euro từ một quốc gia đi chi tiêu tại những nước chấp nhận sử dụng nó, nhưng bạn không thể dùng đồng tiền này trong một cửa hàng ở Mỹ. Tương tự như vậy, với đồng đô la Mỹ, bạn có thể đổi sang hầu hết các loại tiền tệ khác trên thế giới, tuy nhiên bạn không thể vào một cửa hàng ở châu Âu và thanh toán bằng đô la Mỹ.

Trong khi đó, Bitcoin đã đạt được bước tiến xa trong nỗ lực trở thành một loại tiền tệ quốc tế. Điển hình với việc, bạn có thể gửi bitcoin vào ví điện tử khi đang ở châu Âu, sau đó đến một cửa hàng ở Mỹ và thanh toán bằng bitcoin. Bạn có thể giao dịch với các cửa hàng, doanh nghiệp, và các cá nhân trên khắp thế giới bằng bitcoin mà không tốn bất cứ lệ phí giao dịch quốc tế nào hoặc phải đổi bitcoin sang một loại tiền tệ khác.

Càng nhiều doanh nghiệp và người dân chấp nhận bitcoin trên khắp thế giới, thì càng có nhiều khả năng để Bitcoin trở thành một đồng tiền quốc tế chân chính.

Bitcoin và cơ hội trở thành nơi cất trữ giá trị

Bitcoin được tạo ra tương tự như vàng, trong đó mỗi bitcoin đều có giá trị và nguồn cung ứng bitcoin là hữu hạn. Trong khi đó, nguồn cung tiền mặt là vô hạn với hầu hết các loại tiền tệ, điều này giải thích tại sao nảy sinh nhiều vấn đề như đồng tiền Zimbabwe mất giá do chính phủ in thêm quá nhiều tiền.

Có hai lý do chính giải thích tại sao Bitcoin nên được mọi người sử dụng: Thứ nhất, mọi người có thể xem nó như một giải pháp thay thế tiền tệ hiện hành trong các giao dịch tài chính; và thứ hai, mọi người có thể xem nó như một nơi cất trữ giá trị như vàng.

Để trở thành nơi cất trữ giá trị, Bitcoin cần phải đảm bảo được rằng, tình trạng biến động giá sẽ giảm đi, đồng thời giá trị của nó phải ổn định và tăng dần theo thời gian. Ở đây, điều quan trọng không phải là việc các giao dịch được xử lý nhanh chóng hay không, mà là giá trị nó chứa đựng sẽ phải luôn ổn định và bền vững.

Điều này sẽ giúp ích rất lớn cho nhiều người trên khắp thế giới, do những nguyên nhân khách quan, mà không có đủ điều kiện để tiếp cận với các tài khoản ngân hàng hoặc phải dựa vào các tổ chức tài chính ở đất nước họ, vì họ sẽ có khả năng tích trữ tiền tiết kiệm bằng Bitcoin.

Với Bitcoin, nếu một chế độ độc tài lật đổ một quốc gia hoặc phá giá tiền tệ, người dân của đất nước đó sẽ không bị mất hết tiền tiết kiệm mà họ tích lũy được. Nếu họ bỏ chạy tới đất nước khác, họ vẫn có thể tiếp cận được số bitcoin của mình; nói cách khác, họ có thể dễ dàng mang theo khoản tiền tiết kiệm cả đời xuyên biên giới và xuyên quốc gia. Nếu họ phải di dời và bắt đầu cuộc sống ở quốc gia khác, họ sẽ không phải xây dựng lại từ hai bàn tay trắng, bởi vì họ luôn có thể tiếp cận toàn bộ số bitcoin của họ để kiến thiết cuộc sống mới.

Ngay cả đối với những người không phải đối mặt với tình trạng này, thị trường tài chính cùng với các loại tiền tệ thường bất ổn, và Bitcoin có thể cung cấp một sự thay thế khả thi vượt trội hơn vàng với vai trò một nơi cất trữ giá trị. Bất kể Bitcoin có thể thay thế được vàng để trở thành nơi cất trữ giá trị thật sự hay không, thì đối với

nhiều người trên thế giới, Bitcoin đã cung cấp một phương án thay thế ổn định hơn hệ thống tài chính và đồng tiền hiện tại của họ.

Bitcoin tại các nước đang phát triển

Mặc dù nhóm người chấp nhận và sử dụng Bitcoin đầu tiên là các lập trình viên, các nhà lập mã và những người am hiểu kỹ thuật ở các quốc gia giàu có, nhưng trong tương lai, người dùng Bitcoin trong tương lai có thể hoàn toàn ngược lại.

Bitcoin có thể phát huy lợi ích tốt nhất của nó tại nhiều nước đang phát triển, nơi mà hệ thống tài chính và pháp luật tham nhũng, các cơ quan chính phủ được điều hành dưới chế độ độc tài và người dân không tiếp cận được thị trường quốc tế hoặc tài khoản ngân hàng cá nhân.

Trên thế giới, số người sở hữu điện thoại di động đang ngày càng áp đảo số người có tài khoản ngân hàng. Một người sống giữa châu Phi có thể không đủ khả năng tiếp cận được với các dịch vụ ngân hàng, nhưng chỉ với điện thoại di động là họ có thể thiết lập ví Bitcoin và thực hiện giao dịch bằng số bitcoin trong đó.

Hiện thực Walmart, Target hay các nhà bán lẻ khác từ chối Bitcoin không có nghĩa là nó sẽ không nhận được sự chấp nhận từ đa số mọi người trên thế giới. Tương lai của Bitcoin có lẽ không phải là được đón nhận rộng khắp tại Mỹ và châu Âu, mà là ở châu Phi, châu Á và châu Mỹ Latinh.

Trong tương lai, đa số người chấp nhận và sử dụng Bitcoin có thể không phải những lập trình viên máy tính ở độ tuổi 20 tại Thung lũng Silicon, mà là những chủ cửa hàng ở độ tuổi 40 tại châu Phi, sở hữu một chiếc điện thoại thông minh nhưng cả đời chưa bao giờ đụng đến máy tính.

Quy định pháp lý đối với Bitcoin

Ban đầu, Bitcoin bị các chính phủ chỉ trích vì chỉ đem lại ích lợi cho những tên buôn bán ma túy, những tay sát thủ máu lạnh, những kẻ

rửa tiền và nhiều loại tội phạm khác. Lợi ích của Bitcoin là các tính năng mà chính phủ e ngại: các giao dịch tài chính ẩn danh, các khoản thanh toán không thể truy nguyên, khả năng vượt qua sự kiểm soát của chính phủ, và cơ cấu không tồn tại hệ thống kiểm soát hoặc máy chủ trung tâm nào có thể theo dõi nó. Nó có vẻ như mạng lưới thanh toán hoàn hảo cho tội phạm, và tai tiếng của Bitcoin với vai trò phương thức thanh toán trên thị trường ma túy trực tuyến Silk Road đã chứng minh điều này.

Dù thời gian đầu bị nhiều chính phủ chỉ trích hoặc bác bỏ, thì hiện nay, Bitcoin đang bắt đầu được nhiều chính phủ ứng dụng hoặc ít nhất là công nhận. Chẳng hạn, Nhật Bản gần đây đã thông qua điều luật cho phép Bitcoin trở thành phương thức thanh toán hợp pháp trong nước. Nhiều quốc gia khác đã đưa ra quan điểm rằng, việc thiết lập định chế để kiểm soát Bitcoin, chứ không phải cấm đoán nó, là cách tốt nhất để quản lý giao dịch Bitcoin.

Trong khi đó, Coinbase, Kraken, Poloniex, Circle và nhiều công ty khác có cơ chế cho phép đổi các loại tiền tệ pháp định thành tiền mã hóa theo quy định của pháp luật, tương tự như cơ chế kiểm soát đối với các tổ chức tài chính khác.

Hệ thống quy định này đã tước đi nhiều lợi ích của Bitcoin, tuy nhiên, như đã đề cập, những lợi ích bị loại bỏ đó sẽ được thay thế bằng nhiều lợi ích khác mà người dùng cảm thấy quen thuộc và thoải mái hơn.

Hoạt động siết chặt kiểm soát đối với Bitcoin sẽ giúp loại bỏ sợi dây liên kết giữa Bitcoin với các hoạt động tội phạm. Bitcoin càng được nhiều người coi trọng và được điều tiết chặt chẽ hơn, sẽ giúp hoạt động sử dụng bitcoin ngày càng được nhiều chính phủ, doanh nghiệp và công chúng chấp nhận hơn.

Những loại tiền mã hóa riêng biệt và ẩn danh khác

Bitcoin không được thiết kế để nằm trong vòng kiểm soát của các chính phủ hoặc các tổ chức tài chính. Nó được thiết kế để thoát khỏi sự kiểm soát của các chính phủ và các hệ thống tài chính hiện

hành. Khi đồng tiền Bitcoin ngày càng chịu sự kiểm soát chặt chẽ hơn và được tích hợp vào hệ thống tài chính hiện thời nhiều hơn, sẽ có nhiều người tin rằng điều này đi ngược lại hệ tư tưởng ban đầu của Bitcoin.

Hiện nay, xuất hiện hàng trăm loại tiền mã hóa hoạt động tương tự Bitcoin. Nhiều trong số đó đang phát triển những loại ví có tính năng ẩn danh cao hơn và phát triển các giao dịch mang tính riêng tư nhiều hơn.

Trong tương lai, Bitcoin có thể được kiểm soát chặt chẽ và được tích hợp sâu rộng hơn. Điều này sẽ dẫn đến sự gia tăng các loại tiền mã hóa thay thế để cung cấp sự riêng tư cao hơn và hướng đến hoạt động vượt xa vòng kiểm soát của chính phủ.

Bitcoin và nguy cơ bị thay thế bởi Altcoin và các loại tiền mã hóa khác

Bitcoin không phải là loại tiền mã hóa duy nhất có thể sử dụng được cho các giao dịch, mà ngoài nó ra, có hàng trăm lựa chọn khác có khả năng thay thế Bitcoin.

Altcoin là loại tiền mã hóa khác với Bitcoin, chúng là những đồng tiền thay thế được xây dựng dựa trên mã nguồn Bitcoin, sở hữu loại tiền tệ riêng, nhưng hoạt động hoàn toàn độc lập với Bitcoin.

Nhiều Altcoin đã có những bước cải tiến vượt bậc so với Bitcoin, trong khi Bitcoin bị tụt lại phía sau do sự chia rẽ trong mạng lưới về định hướng phát triển trong tương lai. Một ví dụ cho điều này là sự xuất hiện của Litecoin, với thời gian giao dịch nhanh hơn, và khả năng thêm một khối giao dịch mới vào Blockchain chỉ 2,5 phút một lần – nhanh hơn đáng kể khi so với thời gian 10 phút của Bitcoin. Điều này khiến Litecoin trở thành ứng viên sáng giá hơn so với Bitcoin trong nhiều giao dịch tài chính.

Bitcoin Cash là một Altcoin mới được tạo ra trong thời gian gần đây do sự bất đồng về hướng phát triển của Bitcoin trong tương lai. Bitcoin Cash được tạo ra để xử lý các giao dịch với tốc độ nhanh

hơn Bitcoin, và được sử dụng trong các giao dịch diễn ra hằng ngày.

Nếu loại tiền mã hóa như Litecoin hay Bitcoin Cash ngày càng được người tiêu dùng và các doanh nghiệp chấp nhận rộng rãi, thì nó càng có khả năng thay thế Bitcoin để trở thành một loại tiền mã hóa chủ chốt. Cũng có thể các loại tiền mã hóa đó sẽ được sử dụng cho các mục đích đặc biệt hơn Bitcoin, còn Bitcoin có thể vẫn là một loại tiền mã hóa quan trọng được sử dụng cho các giao dịch quy mô lớn. Litecoin, Bitcoin Cash và nhiều Altcoin khác có thể thay thế Bitcoin để được sử dụng cho các giao dịch hằng ngày ở quy mô nhỏ hơn hoặc cho các giao dịch đặc thù ngành.

Bitcoin và nguy cơ trở nên vô giá trị

Hiện nay, Bitcoin ngày càng được chấp nhận nhiều hơn và được tích hợp sâu rộng hơn vào các hệ thống tài chính hiện có. Tuy nhiên, xu hướng này có thể thay đổi. Công nghệ đằng sau tiền mã hóa có thể được áp dụng trong tương lai nhưng Bitcoin có thể không nằm trong viễn cảnh đó.

Các tổ chức tài chính lớn tuổi đời hàng trăm năm như sụp đổ trong một đêm suốt cuộc đại khủng hoảng tài chính. Sự kiện bong bóng hoa tulip ở Hà Lan từ năm 1630 đến năm 1637 xảy ra, giá hoa tulip tăng vọt 5.000% và gấp 10 lần mức lương trung bình thời bấy giờ. Thậm chí, hoa tulip được định giá còn cao hơn mức giá nhà trung bình ở Hà Lan lúc đó. Tuy nhiên, chỉ vài tháng sau đó, giá hoa tulip đã lao dốc thảm hại đến mức gần như bằng 0.

Elliot Prechter, con trai của chuyên viên phân tích thị trường danh tiếng Robert Prechter, đã tuyên bố trên tờ Elliot Wave Theorist rằng chỉ nên mua Bitcoin khi nó đang được giao dịch ở mức 6 xu trong năm 2010. Gần đây, ông còn so sánh sự biến động giá của Bitcoin với sự biến động giá của hoa tulip trong suốt thời kỳ xảy ra bong bóng hoa tulip.

Ông còn đưa ra nhận định về tiềm năng của tiền mã hóa và đánh giá nó như một công nghệ mang tính cách mạng hóa, nhưng những

cuộc cách mạng cũng có thể biến thành cơn cuồng loạn của đám đông. Mạng Internet đã là một dạng công nghệ mang tính cách mạng; tuy nhiên, vẫn diễn ra cơn điên cuồng xoay quanh các công ty Internet, và sàn giao dịch chứng khóan NASDAQ đã tụt xuống khoảng 90% suốt thời kỳ bong bóng dot-com.

Tổng kết chương 11

Tương lai của Bitcoin nói riêng và tiền mã hóa nói chung còn rất khó đoán định được.

Việc Bitcoin có trở thành một phương thức thanh toán được công chúng đón nhận và tin dùng hay không sẽ phụ thuộc thái độ của các doanh nghiệp và người tiêu dùng đối với nó. Trên thực tế, có rất nhiều công ty đã đồng ý đưa Bitcoin trở thành một phương thức thanh toán, nhưng rồi lại gỡ bỏ vì thấy khách hàng không có nhu cầu. Mặc dù Bitcoin và các đồng tiền mã hóa đang ngày càng trở nên phổ biến, nhưng vẫn có nguy cơ xu hướng này bị đảo ngược.

Nếu các công nghệ như mạng Lighting được triển khai, Bitcoin có thể trở thành một giải pháp thanh toán thay thế chính thống và có khi là trở thành một loại tiền tệ quốc tế. Tuy nhiên, như bạn cũng biết, công nghệ thay đổi rất nhanh, nên dù tiền mã hóa hiện là một dạng công nghệ mới nhưng trong tương lai vẫn có thể xuất hiện phương thức thanh toán khác mang tính cách mạng hơn.

Có hàng ngàn các loại tiền mã hóa khác có thể được sử dụng thay thế Bitcoin. Nhiều trong số đó cung cấp những lợi ích và tính năng mà Bitcoin còn thiếu. Đến thời điểm này, có thể nói, Bitcoin là loại tiền mã hóa ra đời đầu tiên, nhưng trong tương lai, vị thế vượt trội của nó có thể bị thay thế.

Elliot Prechter tin rằng công nghệ đằng sau tiền mã hóa sẽ có một tương lai tươi sáng, tuy nhiên, bây giờ vẫn còn quá sớm để biết liệu Bitcoin có thể trở thành Facebook hay MySpace của thế giới tiền mã hóa hay không.

Bảng thuật ngữ

Ghi chú: Bảng thuật ngữ sau đây dựa theo chú giải của Oleg Andreev, nhà thiết kế phần mềm và chuyên gia về Bitcoin.

Địa chỉ (Address)

Một địa chỉ Bitcoin được sử dụng để nhận thanh toán và chuyển bitcoin. Địa chỉ này tương tự một địa chỉ thư điện tử nhưng thay vì nhận thư, bạn nhận được các khoản thanh toán từ người khác.

Địa chỉ có thể khởi tạo miễn phí, dài khoảng 30 ký tự gồm số và chữ.

Địa chỉ khác với ví. Địa chỉ chỉ được sử dụng một lần cho một giao dịch cá nhân để đảm bảo an toàn và bảo mật.

Xem thêm Ví.

Altcoin

Altcoin là viết tắt của “Alternative Coin” (đồng tiền khác) hoặc “Alternative Bitcoin” (Bitcoin khác), được sử dụng để chỉ những loại tiền mã hóa vận hành tương tự Bitcoin nhưng khác biệt với Bitcoin về thời gian xác nhận, Bằng chứng Xử Lý hay các tính năng khác.

Altcoin hầu hết là các phiên bản chỉnh sửa của giao thức Bitcoin, sở hữu khối nguyên thủy riêng và không tương thích với bitcoin. Litecoin là một ví dụ về Altcoin với thời gian xác nhận khối nhanh hơn và hàm dẫn xuất khóa như thuật toán Bằng Chứng Xử Lý.

ASIC

ASIC là viết tắt của thuật ngữ vi mạch tích hợp chuyên dụng (application-specific integrated circuit), là một chip máy tính được đặc biệt thiết kế để vận hành một hay một vài chức năng.

Các chip máy tính phổ biến nhất đều được thiết kế để thực hiện hàng loạt các chức năng và được sử dụng trong máy tính xách tay, máy vi tính, điện thoại thông minh, v.v…

ASIC thường được dùng để chỉ những loại chip

chuyên dụng hoặc toàn bộ các máy móc lắp đặt dựa trên loại chip này được thiết kế để khai thác bitcoin hoặc Altcoin.

ASICMiner xảy ra khi những máy móc này được sử dụng để khai thác trong Bitcoin hoặc Altcoin. Thông thường, ASICMiner tận dụng đồng thời nhiều máy để khai thác trong Bitcoin hoặc Altcoin.

Bit

Bit là một loại đơn vị của bitcoin, tương tự như cent là đơn vị của đô la. Một triệu bit tương đương với 01 bitcoin.

Bitcoin (chữ B in hoa)

Bitcoin với chữ B viết hoa dùng để chỉ mạng lưới thanh toán, giao thức và Blockchain của loại tiền ảo này.

Mạng lưới Bitcoin là toàn bộ các máy tính tuân theo cùng một bộ quy tắc đồng thời trao đổi các giao dịch và các khối với nhau.

Giao thức Bitcoin thiết lập quy chuẩn trong đó mọi thành viên phải tuân thủ để xác nhận giao dịch và yêu cầu người khác kiểm nhận giao dịch của họ.

Mạng lưới Bitcoin là mạng phi tập trung, không tồn tại ngân hàng trung tâm, chính phủ hay tổ chức trung tâm phát hành hay quản lý các giao dịch.

Các giao dịch được xử lý bởi các máy tính trong mạng lưới (theo mô hình ngang cấp – P2P). bitcoin (chữ b viết thường) bitcoin với chữ b viết thường được dùng để chỉ đơn vị bitcoin, chẳng hạn như “gửi 2 bitcoin”.

Tổng số bitcoin được tạo ra được giới hạn trong con số 21 triệu bitcoin.

Bitcoin Unlimited

Mạng lưới Bitcoin xử lý một khối các giao dịch cứ mỗi 10 phút. Còn có hạn định về số giao dịch được đưa vào mỗi khối vì kích thước dữ liệu khối hạn chế.

Kích thước tập tin hiện tại của mỗi khối là 1MB dữ liệu. Khi các giao dịch được đưa vào một khối đạt tới mức 1MB dữ liệu, không một giao dịch nào được thêm vào khối đó nữa và những giao dịch đang chờ xử lý sẽ phải đợi để được thêm vào khối khác.

Bitcoin Unlimited là một đề xuất xóa bỏ kích thước tập tin mỗi khối, cho phép vô số giao dịch được bổ sung vào mỗi khối. Càng nhiều giao dịch được thêm vào mỗi khối, số lần xử lý giao dịch càng tăng.

Có hai đề xuất cải thiện khả năng mở rộng của mạng lưới và tăng tốc độ giao dịch, SegWit và Bitcoin Unlimited.

Bitcoin Unlimited bị từ chối nên một phần của mạng lưới tách ra để thực thi giải pháp này thành một loại tiền mã hóa mới có tên Bitcoin Cash.

SegWit được chấp thuận như một giải pháp để giải quyết vấn đề về khả năng mở rộng trong mạng lưới Bitcoin và sẽ được thực thi trong tương lai gần.

Xem thêm Phân nhánh cứng, Phân nhánh mềm, SegWit.

Khối (Block)

Một khối là một tập hợp các giao dịch được bổ sung vào Blockchain của Bitcoin. Khi một giao dịch được truyền gửi trong mạng lưới Bitcoin, nó sẽ ở trạng thái chờ xử lý cho đến khi được thêm vào một khối trong Blockchain. Ngay khi một giao dịch được nạp vào một khối đã được chấp thuận trên Blockchain, giao dịch đó được xử lý.

Các khối chứa giao dịch mới cùng với tiêu đề khối, giao dịch, nhãn thời gian, bằng chứng xử lý và hồ sơ của khối liền trước trên Blockchain.

Các giao dịch và dữ liệu trong một khối không thể bị sửa đổi hoặc xóa bỏ, một khi khối được thêm vào Blockchain, nó sẽ trở thành hồ sơ dữ liệu và giao dịch vĩnh cửu. Mỗi khối chứa thông tin về khối liền trước, từ đó tạo nên một chuỗi liên kết các khối không thể sửa đổi.

Các khối được đưa vào Blockchain thông qua quá trình khai thác. Các thợ đào giải mảnh ghép toán học Bằng Chứng Xử Lý để thêm được một khối vào Blockchain, họ nhận được phần thưởng khối bằng bitcoin vì đã giải quyết được vấn đề khó khăn này và bổ sung một khối hợp lệ vào Blockchain. Phần thưởng khối này nhằm khuyến khích đóng góp nguồn lực và công suất tính toán vào mạng lưới Blockchain.

Trong Blockchain của Bitcoin, một khối giao dịch mới được bổ sung vào theo chu kỳ 10 phút một lần.

Công cụ khám phá khối Block Explorer

Công cụ Block Explorer cho phép bạn khám phá tất cả các giao dịch đã và đang diễn ra trên một Blockchain cụ thể.

Ví dụ, tại blockchain.info, bạn có thể quan sát các giao dịch đang diễn ra hoặc tìm hiểu các giao dịch trước đó trên Blockchain của Bitcoin.

Chiều cao khối (Block Height) Chiều cao khối là số của một khối trên Blockchain. Chiều cao khối bằng 0 tức là khối đầu tiên, hay còn gọi là Khối Nguyên thủy trên Blockchain. Chiều cao khối bằng 1 tức là khối sau Khối Nguyên thủy.

Mỗi khối được thêm vào trên Blockchain có chiều cao khối lớn hơn khối trước nó 1 đơn vị.

Phần thưởng khối (Block Reward)

Phần thưởng khối được trao cho thợ đào đã bổ sung thành công một khối các giao dịch vào Blockchain.

Phần thưởng được trả bằng bitcoin cho thợ đào. Phần thưởng khối Bitcoin giảm theo thời gian cho đến khi không còn phần thưởng khối Bitcoin nào nữa. Quá trình này được gọi là chia đôi, vì phần thưởng khối giảm đi một nửa sau mỗi 210.000 khối.

Phần thưởng khối giúp khuyến khích các thợ đào đóng góp công suất tính toán vào mạng lưới, nhờ đó tăng cường độ bảo mật và công suất xử lý, tạo nên một mạng lưới an toàn và nhanh chóng hơn.

Blockchain

Blockchain là cơ sở dữ liệu căn bản của mạng lưới Bitcoin. Nó là một sổ cái phân tán chung, công khai gồm tất cả các giao dịch đã được xác nhận.

Mỗi khối được thêm vào Blockchain chứa một nhóm các giao dịch cùng với dữ liệu như một chỉ dẫn tới khối liền trước trên Blockchain.

Bằng cách chỉ dẫn tới khối liền trước, các khối liên kết với nhau tạo thành một chuỗi. Chính từ đây, cái tên Blockchain (chuỗi các khối) ra đời.

Trên mạng lưới Bitcoin, mọi người đều có thể quan sát các giao dịch và các khối trên Blockchain tới tận khối đầu tiên, hay còn gọi là Khối Nguyên thủy. Blockchain của Bitcoin có thể được quan sát bằng cách sử dụng công cụ Block Explorer.

Các khối được thêm vào Blockchain thông qua quá trình khai thác. Các giao dịch chưa được xác nhận chờ xử lý sẽ không được thêm vào Blockchain cho đến khi chúng được đưa vào một khối.

Xem thêm Block Explorer, Khối Nguyên thủy, Khai thác, Giao dịch chưa xác nhận.

BTC

BTC là mã tiền tệ của 01 Bitcoin, tương tự như USD của đô la Mỹ hay các mã tiền tệ khác.

Giao dịch Coinbase (Coinbase transaction)

Một tập lệnh đầu vào của một giao dịch mà giao dịch đó khởi tạo bitcoin mới, hoặc tên của chính giao dịch đó (giao dịch Coinbase). Giao dịch Coinbase không tiêu dùng bất cứ giao dịch hiện hành nào, mà chỉ chứa một đầu vào có thể bao hàm mọi loại dữ liệu trong tập lệnh của nó.

Một số vùng khai thác đưa tên của mình vào các giao dịch Coinbase (vì thế mọi người có thể ước lượng công suất băm mỗi vùng tạo được là bao nhiêu).

Giao dịch Khối Nguyên thủy của Bitcoin chứa chỉ dẫn tới bài báo đăng ngày 03/01/2009 trên tạp chí Times để chứng tỏ rằng không có khối nào được khởi tạo trước ngày đó.

Giao dịch Coinbase còn được sử dụng để bầu chọn một thay đổi giao thức (chẳng hạn như P2SH). Các thợ đào bầu chọn bằng cách đưa dấu hiệu đồng ý vào trong Coinbase rồi xem có bao nhiêu thành viên ủng hộ sự thay đổi.

Kho lạnh (Cold Storage)

Kho lạnh là các biện pháp bảo mật được áp dụng để bảo vệ tiền mã hóa và khóa cá nhân khỏi bị tấn công.

Kho lạnh có thể đòi hỏi một máy tính không kết nối Internet, ví phần cứng chuyên dụng, USB có kèm tập tin ví, hay ví giấy.

Giao dịch đã được xác nhận (Confirmed Transaction)

Một giao dịch đã được xác nhận là một giao dịch đã được kiểm nhận và xử lý trên mạng lưới Bitcoin rồi bao hàm trong một khối trên Blockchain.

Ngay khi một giao dịch được xác nhận trên mạng lưới Bitcoin, nó sẽ không thể bị thu hồi. Chính xác hơn, số lượng xác nhận của giao dịch sẽ quyết định khả năng giao dịch bị từ chối hay đảo chiều.

Xem Số xác nhận.

Số xác nhận (Confirmation Number)

Số lượng xác nhận cho thấy khả năng một giao dịch có thể bị từ chối hay đảo chiều trên Blockchain của Bitcoin.

Giao dịch có 0 xác nhận đồng nghĩa với việc giao dịch đó không được xác nhận (trong bất cứ khối nào).

Một xác nhận tức là giao dịch được thêm vào khối mới nhất trong chuỗi chính.

Hai xác nhận cho biết giao dịch được đưa vào khối liền trước khối mới nhất trên Blockchain.

Số lượng xác nhận càng cao, khả năng giao dịch bị từ chối hoặc đảo chiều càng thấp.

Nhiều công ty chấp nhận Bitcoin như một phương thức thanh toán sẽ đòi hỏi tối thiểu 6 xác nhận làm bằng chứng rằng giao dịch sẽ không bị đảo chiều trước khi coi giao dịch đó là hợp lệ.

Tiền mã hóa (Cryptocurrency)

Tiền mã hóa là một loại tiền kỹ thuật số không được phát hành hay chịu sự quản lý của chính phủ, ngân hàng trung ương, hoặc các tổ chức trung ương khác.

Từ tiền mã hóa (cryptocurrency) được tạo ra bằng cách ghép hai từ mật mã học (cryptography) và tiền tệ (currency). Tiền mã hóa vận hành thông qua ứng dụng toán học mật mã và các kỹ thuật mã hóa.

Hàm băm mật mã học (Cryptographic Hash Function)

Một hàm băm mật mã học sẽ mã hóa dữ liệu để nó gần như không thể giải mã được nếu không có quyền truy cập.

Độ dài thông tin xuất của dữ liệu được mã hóa sẽ như nhau, bất kể một từ hay cả một cuốn tiểu thuyết được mã hóa. Dữ liệu xuất có độ dài bất biến này được gọi là “mã băm” của dữ liệu.

Mọi thay đổi trên dữ liệu nhập, chẳng hạn như từ viết thường chuyển thành in hoa, đều sẽ tạo nên dữ liệu xuất hoàn toàn khác.

Mã băm đầu ra xuất hiện ngẫu nhiên và vì thế gần như không thể cố gắng xác định dữ liệu đầu vào được sử dụng để tạo ra mã băm đó.

Mật mã học (Cryptography)

Mật mã học là một lĩnh vực toán học xoay quanh việc mã hóa, an ninh và bảo mật dữ liệu. Mật mã học là công nghệ nền tảng của tiền mã hóa, chẳng hạn như Bitcoin, cho phép thực hiện các hoạt động sáng tạo, quản lý và bảo vệ mạng lưới cũng như các giao dịch.

Độ khó (Difficulty)

Độ khó là thước đo mức độ khó khăn của việc thêm khối mới vào Blockchain của Bitcoin.

Chỉ tiêu độ khó của mạng lưới Bitcoin là chỉ tiêu tối đa chia cho chỉ tiêu hiện tại. Độ khó của mạng lưới Bitcoin được điều chỉnh sau mỗi 2.016 khối dựa theo thời gian dùng để xác thực 2.016 khối trước đó.

Độ khó được điều chỉnh trên mạng lưới Bitcoin để duy trì thời gian thêm khối vào Blockchain là 10 phút một lần.

Độ khó mạng lưới Bitcoin được dự đoán sẽ tăng từ 3-5% sau mỗi hai tuần. Tại thời điểm viết cuốn sách này, độ khó của mạng Bitcoin là 804.525.194.568.

Độ sâu (Depth)

Độ sâu cho biết vị trí của một giao dịch trên Blockchain. Một giao dịch với 6 xác nhận còn có thể gọi là “độ sâu 6 khối”.

Độ sâu của một giao dịch trong Blockchain càng lớn, độ tin cậy và tín nhiệm của giao dịch đó càng cao.

Xem thêm Số xác nhận.

Giao dịch lặp chi (Double Spending)

Giao dịch lặp chi xảy ra khi cùng một số bitcoin được gửi hai lần. Khi một giao dịch được truyền gửi trên mạng lưới Bitcoin, trước tiên, nó sẽ ở trong tình trạng chờ xử lý hoặc chưa xác nhận.

Nếu bạn có 5 bitcoin trong ví và bạn gửi cho người khác 5 bitcoin, giao dịch đó sẽ chờ xử lý cho đến khi nó được thêm vào một khối. Trong khi giao dịch đó chờ xử lý, nếu bạn lại gửi 5 bitcoin đó cho người khác nữa, giao dịch này sẽ tiếp tục trong tình trạng chờ xử lý. Đây được gọi là giao dịch lặp chi, khi bạn cố gửi hai lần cùng một số bitcoin.

Giao dịch lặp chi không dễ xảy ra trên mạng lưới Bitcoin, vì mạng lưới sẽ chỉ tạm coi cả hai giao dịch đều hợp lệ. Tuy nhiên, ngay khi một trong hai giao dịch được đưa vào mạng lưới Bitcoin, nó vào trạng thái đã xác nhận còn giao dịch kia sẽ bị từ chối.

Càng nhiều khối được thêm vào trên khối chứa giao dịch đó, khả năng giao dịch lặp chi được số bitcoin đó càng khó khăn. Mỗi khối được thêm vào trên nó được coi là một xác nhận rằng giao dịch đó hợp lệ và không thể bị đảo chiều.

Tấn công Quá bán là tình huống khi một ai đó nắm quyền kiểm soát trên 50% mạng lưới Bitcoin và giao dịch lặp chi bitcoin có thể xảy ra.

Xem thêm Tấn công Quá bán.

Ethereum

Ethereum là nền tảng cho phép các ứng dụng phi tập trung, phân tán và hợp đồng thông minh vận hành trên một máy ảo bên trên Blockchain.

Mạng lưới Ethereum sử dụng đồng tiền mã hóa ether cho hoạt động thanh toán trên mạng lưới. Ether được trao đổi để vận hành các ứng dụng phi tập trung trên mạng lưới.

Ether là đồng tiền mã hóa lớn thứ hai trên thế giới, với giá trị vốn hóa thị trường hơn 20 tỷ đô la chỉ đứng sau Bitcoin.

Các ứng dụng phi tập trung (dApp) không có máy chủ trung tâm, người dùng kết nối với những người khác theo mô hình ngang cấp.

Các hợp đồng thông minh là loại hợp đồng chạy trên nền tảng Ethereum. Chúng được viết bằng mã máy tính để tự động xác nhận, thực thi và thúc ép thực hiện các điều khoản hợp đồng.

Sàn giao dịch

Sàn giao dịch là thị trường trao đổi và giao dịch tiền mã hóa hoặc tiền pháp định. Có nhiều sàn giao dịch tiền mã hóa lớn với nhiều tính năng và tiền tệ khả dụng. Một trong những sàn giao dịch nổi tiếng nhất là Kraken, Poloniex và Bittrex.

Tiền pháp định

Tiền pháp định là loại tiền được một chính phủ tuyên bố là hợp pháp, ngay cả khi nó không được bảo đảm bằng vàng hay tài sản hữu hình.

Tiền đô la Mỹ, euro và gần như mọi loại tiền do chính phủ phát hành đều là ví dụ về tiền pháp định.

Trước khi có tiền pháp định, các quốc gia thường bảo chứng tiền tệ của họ theo vàng, bạc hoặc tài sản khác, chẳng hạn như tờ 1 bảng có thể quy đổi sang 01 pound kim loại bạc.

Phân nhánh (Fork)

Phân nhánh trong tiền mã hóa cho thấy sự phân tách trong mã nguồn của Blockchain. Khi hai khối được tạo ra cùng lúc (cùng chiều cao), sự phân nhánh xuất hiện.

Mạng lưới Blockchain được thiết kế để ứng phó với tình trạng phân nhánh, mạng lưới thường sẽ chọn khối có độ khó lớn nhất rồi thêm nó vào Blockchain với tư cách khối hợp lệ tiếp theo.

Xem thêm Phân nhánh Cứng và Phân nhánh Mềm.

Phân nhánh Cứng (Hard Fork)

Phân nhánh cứng là tình trạng chia rẽ vĩnh viễn trong Blockchain. Tình trạng này thường xảy ra khi các nút chưa cập nhật không thể xác thực các khối được tạo ra bởi các nút cập nhật tuân theo quy tắc đồng thuận mới.

Một số người sử dụng thuật ngữ Phân nhánh Cứng khi đề cập tới một sự thay đổi trong giao thức mà cần tới sự đồng thuận của đa số rất lớn thành viên nhưng một phần đáng chú ý trong mạng lưới vẫn tiếp tục sử dụng Blockchain ban đầu và giao thức cũ.

Một ví dụ của Phân nhánh Cứng là sự kiện phân nhánh cứng Ethereum vào tháng Bảy năm 2016, giao thức đã được sửa đổi nhưng một phần đáng kể thành viên vẫn theo quy ước cũ, từ đó hình thành nên Ethereum Classic và Ethereum để vận hành với tư cách hai Blockchain riêng biệt.

Một phân nhánh cứng có thể được coi tương tự như một bản cập nhật phần mềm trong đó có nhiều thay đổi về hệ thống và bạn phải cập nhật phần mềm mới có thể tiếp tục sử dụng nó.

Sự kiện thay đổi mới nhất trong mạng lưới Bitcoin khi triển khai SegWit là ví dụ về phân nhánh mềm.

Phân nhánh Mềm (Soft Fork)

Phân nhánh mềm là sự thay đổi trong giao thức Blockchain mà khối/giao dịch hợp lệ liền trước bị liệt kê là không hợp lệ.

Phân nhánh mềm là tình trạng tương thích ngược, các nút cũ không cập nhật sẽ coi các khối mới là hợp lệ. Loại phân nhánh này chỉ đòi hỏi đa số thợ đào đã cập nhật thực thi các quy định mới.

Một phân nhánh mềm có thể được coi tương tự như một phiên bản cập nhật phần mềm trong đó có nhiều thay đổi về hệ thống nhưng bạn không cần cập nhật phần mềm mà vẫn có thể tiếp tục sử dụng nó.

Xem thêm Phân nhánh và Phân nhánh Cứng.

Khối Nguyên thủy (Genesis Block)

Khối nguyên thủy là khối đầu tiên trên một Blockchain.

Trong Blockchain của Bitcoin, Khối Nguyên thủy ra đời vào ngày mùng ba tháng Một năm 2009 và trong Coinbase của nó có chứa trích dẫn với nội dung: “Tờ Times ngày 03/01/2009, Đại Pháp quan đứng bên bờ vực phải viện trợ ngân hàng lần thứ hai”. Đây là bằng chứng cho thấy không tồn tại các khối được bí mật đào trước ảnh hưởng tới Blockchain trong tương lai.

Thông điệp còn ám chỉ tới lý do cho sự tồn tại của Bitcoin: Tình trạng lạm phát tiền bạc liên miên do chính phủ và ngân hàng gây ra.

Chia đôi (Halving)

Chia đôi là sự kiện giảm một nửa số phần thưởng khối mà các thợ đào nhận được khi kiểm nhận các giao dịch. Trong mạng Bitcoin, phần thưởng giảm một nửa sau mỗi 210.000 khối (khoảng 4 năm một lần).

Vì từ Khối Nguyên thủy tới khối 209999 vào tháng Mười Hai năm 2012, phần thưởng khối là 50 BTC, nên cho tới trước năm 2016 là 25 BTC, rồi giảm xuống 12,5 BTC và cứ thế cho đến lần chia đôi cuối cùng vào năm 2140; sau đó trở đi, sẽ không có bitcoin nào được tạo ra nữa.

Vì tình trạng chia đôi phần thưởng khối, nên tổng cung bitcoin được giới hạn trong con số khoảng 21 triệu bitcoin.

Công suất băm (Hashrate)

Công suất băm là sức xử lý của phần cứng khai thác trên một mạng lưới tiền mã hóa.

Vào thời điểm viết cuốn sách này, tổng công suất băm của tất cả các thợ đào trong mạng lưới Bitcoin là 3.572.757 terahash mỗi giây (hàng nghìn tỷ hash* mỗi giây). Tức là khoảng 3.572.757 nghìn tỷ tính toán được thực hiện mỗi giây trên toàn mạng lưới.

* Đơn vị đo lường công suất băm. (BTV)

Litecoin

Litecoin là một trong những loại tiền mã hóa lớn mạnh nhất và phổ biến nhất. Nó thay đổi trong khoảng vị trí thứ 4 và thứ 5 trong danh sách tiền mã hóa lớn nhất, căn cứ theo giá trị vốn hóa thị trường. Tại thời điểm viết cuốn sách này, giá trị vốn hóa thị trường của Litecoin vào khoảng 2 tỷ đô.

Litecoin được xây dựng dựa trên thuật toán Bằng chứng Xử lý dùng hàm dẫn xuất khóa. Mạng lưới Litecoin có thể xử lý giao dịch nhanh hơn mạng Bitcoin, vì thời gian tạo khối của Litecoin là 2,5 phút trong khi của Bitcoin là 10 phút.

Litecoin nhận được đông đảo sự công nhận như một hình thức thanh toán trong môi trường trực tuyến. Nếu bitcoin được coi là đồng tiền mã hóa vàng thì litecoin có thể đạt danh hiệu đồng tiền mã hóa bạc.

Chuỗi chính (Main Chain)

Chuỗi chính là Blockchain chính, là dãy các khối kết nối với nhau dài nhất tính từ khối nguyên thủy tới khối mới nhất.

Khai thác (Mining)

Khai thác là quá trình thêm khối mới vào Blockchain của Bitcoin để đổi lấy phần thưởng khối và phí giao dịch.

Các thợ đào tập trung công suất tính toán và nguồn lực vào việc giải quyết các mảnh ghép toán học để thêm khối vào Blockchain. Mảnh ghép toán học mà thợ đào giải đáp được gọi là bằng chứng xử lý.

Khai thác Bitcoin là quá trình sử dụng phần cứng máy tính để thực hiện các bài toán để xác nhận giao dịch. Các thợ đào thu được phí giao dịch và được thưởng bitcoin cho mỗi giao dịch họ xác nhận.

Xem thêm Vùng Khai thác, Thợ đào, Phần thưởng Khối, Bằng chứng Xử lý.

Vùng khai thác (Mining Pool)

Vùng khai thác là một nhóm người hoặc tập hợp các máy tính góp công suất tính toán và nguồn lực lại với nhau để khai thác khối. Phần thưởng khối và phí giao dịch được phân chia căn cứ theo công suất tính toán mà mỗi thành viên đóng góp.

Xác suất để thêm một khối vào Blockchain phụ thuộc vào công suất tính toán. Các thợ đào cá nhân nhỏ lẻ có thể làm việc suốt nhiều tháng mới nhận được một phần thưởng khối. Các vùng khai thác giúp tạo nên nguồn thu dù nhỏ nhưng ổn định hơn nhờ việc kết hợp công suất tính toán lại với nhau.

Thợ đào (Miner)

Một người, một phần mềm hoặc một phần cứng thực hiện hoạt động khai thác.

Đa chữ ký (Multi-Signature/multisig)

Các địa chỉ đa chữ ký yêu cầu nhiều hơn một khóa để phê chuẩn giao dịch từ địa chỉ đó.

Địa chỉ đa chữ ký có thể đòi hỏi số lượng chữ ký bất kỳ để ủy quyền giao dịch, nhưng chủ yếu là hai chữ ký.

Số lượng chữ ký cần để xác thực được thiết lập khi địa chỉ được khởi tạo.

Các địa chỉ đa chữ ký ít bị tội phạm tấn công hơn.

Tham số Nonce

Là viết tắt của “số dùng một lần” (number used once), số này được đưa vào tiêu đề của khối được thêm vào Blockchain.

Tham số Nonce là số ngẫu nhiên và liên tục được thay đổi để tìm ra số tạo được mã băm hợp lệ trong suốt quá trình giải đáp Bằng chứng Xử lý.

Mỗi khi tham số Nonce được thay đổi, mã băm của tiêu đề khối đều được tính toán lại.

Một tham số Nonce hợp lệ là số mà các thợ đào phải tìm ra để thêm được một khối hợp lệ vào Blockchain của Bitcoin.

Xem thêm Khai thác, Bằng chứng Xử lý, Tiêu đề Khối.

Ví giấy (Paper Wallet)

Ví giấy là một phương pháp bảo quản tiền mã hóa ngoại tuyến, là một hình thức của kho lạnh trong đó khóa cá nhân của địa chỉ ví được in ra trên một mảnh giấy.

Để truyền gửi bitcoin, một khóa phải được nhập vào ứng dụng ví, vì thế nó có thể ký nhận một giao dịch.

Mô hình ngang cấp (Peer-to-Peer/P2P)

Mô hình ngang cấp là mô hình trong đó các thành viên trong mạng lưới giao dịch trực tiếp với nhau mà không cần đến hệ thống tập trung hay tổ chức trung gian.

Paypal là một ví dụ về tổ chức trung gian với nhiều giao dịch điện tử, vì mỗi giao dịch được truyền gửi khắp hệ thống tập trung của Paypal

và được hệ thống này hỗ trợ.

Bitcoin là dẫn chứng về mạng lưới ngang cấp vì không tồn tại máy chủ trung tâm hay tổ chức trung gian trong nó. Mọi thành viên của mạng lưới Bitcoin giao dịch trực tiếp với nhau.

Khóa cá nhân (Private Key)

Khóa cá nhân là một đoạn mã ứng dụng mật mã học cung cấp cho bạn quyền truy cập một ví Bitcoin.

Cũnhg như mã PIN cho bạn quyền tiếp cận khoản tiền trong ngân hàng khi kết hợp với thẻ ngân hàng của bạn, khóa cá nhân trao cho bạn khả năng tiếp cận tiền trong ví Bitcoin.

Bạn nên giữ bía mật khóa cá nhân như bạn giữ bí mật mã PIN của mình và đừng chia sẻ với ai nếu không họ sẽ có thể truy cập bitcoin của bạn.

Khóa công khai (Public Key)

Khóa công khai cũng tương tự như số tài khoản ngân hàng của bạn. Một địa chỉ Bitcoin là bản mã hóa khóa công khai của bạn. Khi kết hợp khóa công khai với khóa cá nhân, bạn có thể tiếp cận số tiền trong ví Bitcoin của mình.

Bạn có thể chia sẻ khóa cá nhân để nhận tiền gửi tới ví, nhưng để truy cập ví, bạn phải kết hợp nó với khóa cá nhân.

Chia sẻ địa chỉ Bitcoin để nhận tiền sẽ an toàn hơn so với khóa công khai không được mã hóa của bạn.

Xem thêm Địa chỉ.

Bằng chứng Xử lý (Proof-of-Work/PoW)

Bằng chứng Xử lý là lời giải cho mảnh ghép toán học cần được đưa ra để thêm một khối vào Blockchain.

Mảnh ghép này rất khó giải đáp nhưng lại rất dễ xác nhận xem có đúng hay không. Hãy tưởng tượng nó như mật mã cho một ổ khóa, sẽ rất khó đoán mật mã khóa là gì, nhưng một khi phát hiện ra, mọi người đều rất dễ dàng kiểm tra xem mật mã đó có mở được khóa không.

Các khối mới không thể được đưa vào Blockchain của Bitcoin nếu chúng không chứa đáp án chính xác cho mảnh ghép toán học này. Mảnh ghép này là một con số (tham số Nonce) mà khi kết hợp với dữ liệu trong một khối, nó sẽ tạo ra mã băm thấp hơn chỉ tiêu của mạng lưới.

Cần rất nhiều công suất tính toán, điện năng và nguồn lực mới có thể tạo ra bằng chứng xử lý trên mạng lưới Bitcoin. Có nhiều phương án thay thế Bằng chứng Xử lý đã được nhiều mạng tiền mã hóa khác ứng dụng như Bằng chứng Cổ phần và Bằng chứng Hoạt động.

Xem thêm Khai thác, Tham số Nonce, Bằng chứng Hoạt động, Bằng chứng Cổ phần.

Bằng chứng Hoạt động (Proof of Authority/PoA)

Bằng chứng Hoạt động là giải pháp thay thế cho Bằng chứng Cổ phần và Bằng chứng Xử lý.

Trong hệ thống Bằng chứng Hoạt động, quyền ra quyết định được phân bổ cho những cá nhân cụ thể trong mạng lưới Blockchain. Những người này sở hữu khóa cá nhân đặc biệt cho phép họ khởi tạo giao dịch và khối trên Blockchain.

Bằng chứng Cổ phần (Proof of Stake/PoS)

Bằng chứng Cổ phần là giải pháp thay thế cho hệ thống Bằng chứng Hoạt động và Bằng chứng Xử lý.

Bằng chứng Cổ phần là quá trình trong đó lượng tiền mã hóa một cá nhân sở hữu sẽ quyết định lượng khai thác của cá nhân đó. Một người sở hữu 1% tiền mã hóa được khai thác 1% khối.

Hệ thống Bằng chứng Xử lý cần rất nhiều công suất tính toán và điện năng mới có thể thêm khối vào Blockchain. Những nguồn lực này chỉ được sử dụng để chứng minh rằng thợ đào đã đóng góp nguồn lực vào mạng lưới. Vì thế, để vận hành hệ thống Bằng chứng Xử lý trên quy mô lớn như mạng lưới Bitcoin sẽ cực kỳ tốn kém và lãng phí.

Bằng chứng Cổ phần hoạt động trên giả định một người sở hữu cổ phần tiền mã hóa sẽ không muốn cổ phần của họ mất giá vì thế sẽ hành động vì lợi ích cao nhất của họ trong mạng lưới. Bằng chứng Cổ phần yêu cầu ít công suất tính toán và nguồn lực hơn Bằng chứng Xử lý.

Peercoin là đồng tiền ảo đầu tiên sử dụng Bằng chứng Cổ phần. Ethereum hiện đang ứng dụng Bằng chứng Cổ phần trên quy mô nhỏ hơn, song song với Bằng chứng Xử lý.

Mã QR (QR Code)

Mã QR tương tự như mã vạch, trong đó dữ liệu như địa chỉ trang web hay địa chỉ Bitcoin được lập mã và hiển thị dưới dạng ảnh vuông. Mã QR có thể được quét và giải mã bằng các ứng dụng đọc mã kết hợp với máy quét hoặc máy ảnh của điện thoại.

Satoshi

Một Satoshi là lượng Bitcoin nhỏ nhất. Cứ 01 Satoshi tương ứng với 0,00000001 bitcoin. Cái tên Satoshi được dùng để vinh danh người sáng tạo ra Bitcoin: Satoshi Nakamoto.

Satoshi Nakamoto

Satoshi Nakamoto là bút danh của người sáng tạo ra đồng Bitcoin. Vào thời điểm cuốn sách này được viết ra, danh tính thật sự của Satoshi Nakamoto vẫn là một ẩn số.

Satoshi Nakamoto có thể là một cá nhân hay một nhóm người. Có rất nhiều giả thuyết về vị sáng lập viên Bitcoin này, nhưng không có bằng chứng rõ ràng về người đó.

Tiêu đề bài báo trong Khối Nguyên thủy trên Blockchain của Bitcoin lấy từ một tờ báo của Vương quốc Anh. Điều này khiến nhiều người cho rằng Sa-toshi Nakamoto đã sống tại Anh vào năm 2009 khi khối đầu tiên của Blockchain Bitcoin được khai thác.

Nhân chứng tách rời (Segregated Witness/ SegWit)

Đây là phiên bản cập nhật được đề xuất cho phần mềm Bitcoin (và Litecoin) để cải thiện khả năng mở rộng và tốc độ xử lý giao dịch.

Đây là sự phân nhánh mềm, trong đó hướng tới việc tiết giảm kích thước khối để giúp nhiều giao dịch được nhận vào khối hơn. Mỗi giao dịch trong Bitcoin chứa thông tin người gửi, người nhận và chữ ký số. Chữ ký số là “nhân chứng” của giao dịch cho biết người gửi có quyền gửi số tiền đó.

Chữ ký số đóng vai trò quan trọng nhưng lại tốn nhiều dung lượng và chỉ được sử dụng vào lúc giao dịch được xử lý. SegWit đề xuất tách rời chữ ký ra khỏi giao dịch để giảm kích thước dữ liệu và cho phép nhiều giao dịch được đưa vào khối hơn.

SegWit đã được tán thành và sẽ được triển khai trong tương lai. Bitcoin Unlimited là một đề xuất phân nhánh cứng đã bị từ chối.

Xem thêm Phân nhánh, Phân nhánh Mềm, Bitcoin Unlimited.

Thuật giải băm an toàn (Secure Hash Algorithm/SHA)

Thuật giải băm an toàn là một hàm băm mật mã học được Viện Tiêu chuẩn và Kĩ thuật Quốc gia Mỹ (NIST) tạo ra như một Tiêu chuẩn Xử lý Thông tin Liên bang Mỹ (FIPS).

Thuật giải băm an toàn là phương thức trong đó ngay khi dữ liệu được mã hóa bằng SHA, nó gần như bất khả giải đối với những ai không có quyền truy cập.

Xem thêm Hàm băm mật mã học và SHA256.

SHA 256

SHA 256 là thuật giải băm an toàn được sử dụng trong hệ thống Bằng chứng Xử lý của Bitcoin. Thuật giải băm SHA 256 sinh ra các mã băm ổn định 256 bit (32 byte) độc nhất.

Chữ ký (Signature)

Chữ ký trong mạng lưới Bitcoin là phương thức toán học nhằm chứng minh quyền sở hữu bitcoin trong ví và quyền thực hiện giao dịch.

Trong Bitcoin, khóa cá nhân phải kết hợp với khóa công khai để ký một giao dịch. Mạng lưới Bitcoin có thể xác thực rằng khóa cá nhân và khóa công khai phù hợp với một chữ ký được sử dụng trong giao dịch, đồng thời vẫn giữ bí mật khóa cá nhân.

Bitcoin sử dụng giải thuật Ký Số Hệ Mật Đường Cong Elliptic (ECDSA) để ký các giao dịch.

Chỉ tiêu (Target)

Một số 256-bit đặt ra giới hạn trên về tính hợp lệ cho một mã băm của tiêu đề khối. Chỉ tiêu càng thấp, độ khó trong việc tìm ra mã băm hợp lệ càng cao. Chỉ tiêu tối đa (dễ nhất) là 0x00000000F FFF0000000000000000000000000000000000000000000000000000.

Độ khó và chỉ tiêu được điều chỉnh sau mỗi 2.016 khối (xấp xỉ 2 tuần) để duy trì khoảng thời gian giữa các khối là gần 10 phút.

Phí giao dịch (Transaction Fees)

Phí giao dịch là phí được trả cho một thợ đào vì đã thêm giao dịch vào một khối. Phí giao dịch khác với phần thưởng khối, phí giao dịch không bắt buộc nhưng lại giúp tăng tốc độ và mức ưu tiên của một giao dịch.

Thợ đào, người băm thành công một khối giao dịch, sẽ được nhận toàn bộ phí giao dịch cho các giao dịch được thêm vào khối đó.

Giao dịch chưa được xác nhận (Unconfirmed Transactions)

Giao dịch chưa được xác nhận là một giao dịch chưa được đưa vào trong bất cứ khối nào. Các giao dịch chưa được xác nhận sẽ vẫn trong trạng thái chưa được xác nhận cho đến khi mạng lưới thêm chúng vào Blockchain hoặc từ chối chúng. Một giao dịch chưa được xác nhận còn có tên là giao dịch “0 xác nhận”.

Xem thêm Số Xác nhận.

Ví (Wallet)

Ví là nơi bạn lưu trữ khóa cá nhân để truy cập số dư tiền mã hóa của bạn (chẳng hạn như bitcoin). Ví không chứa tiền mã hóa mà chứa các khóa để tiếp cận và truyền gửi chúng. Tiền mã hóa thật sự được ghi chép và lưu trữ trong Blockchain.

Ví Web (Web Wallet)

Một dịch vụ web cung cấp chức năng ví: Khả năng lưu trữ, truyền gửi và thu nhận bitcoin. Điều quan trọng là phải đặt nhiều niềm tin vào công ty và dịch vụ ví web. Việc thiết lập một ví web dễ dàng đến nỗi nhiều trong số chúng có nguy cơ bị tấn công hoặc gian lận cao. Ví web đáng tin cậy và an toàn nhất đối với bitcoin hiện nay là Blockchain.info.

Các sàn giao dịch trực tuyến cũng cung cấp chức năng ví, vì thế các sàn này có thể được sử dụng như ví web. Nhưng rất không nên tích trữ nhiều tiền mã hóa trong một ví web.

XBT

Một mã tiền tệ không chính thống cho 01 bitcoin. BTC và XBT là hai mã phổ biến được sử dụng để chỉ 01 bitcoin.

Xem thêm BTC.

Tấn công Quá bán (51% Attack)

Tấn công Quá bán còn được gọi là “tấn công giao dịch lặp chi” hoặc “tấn công trên 50%”.

Tấn công Quá bán xảy ra khi trên 50% công suất tính toán của mạng lưới Bitcoin bị một người hoặc một nhóm người kiểm soát.

Mạng lưới Bitcoin vận hành dựa trên sự đồng thuận của đa số thành viên, vì thế khi kiểm soát được hơn 50% công suất tính toán toàn mạng lưới, kẻ gian có thể xác nhận hoặc từ chối nhiều giao dịch, thao túng giao dịch và lặp chi bitcoin.

Càng nhiều thợ đào và công suất tính toán được đóng góp vào mạng lưới, càng khó xảy ra Tấn công Quá bán.

Tấn công Quá bán không thể thực hiện trên mạng lưới Bitcoin, nhưng lại khả thi ở nhiều mạng lưới tiền mã hóa mới ra đời và quy mô nhỏ hơn.

Tài liệu tham khảo

1. Mathematics and Measurement, tác giả O.A.W Dilke, 1987

2. A Brief History of Workers’ Compensation, tác giả Gregory P. Guyton, 1999

3. Forty centuries of wage and price controls, tác giả Schuettinger, Robert L. & Butler, Eamonn F., 1979

4. Kinh Thánh, bản của vua James, Cách ngôn 20:10, New American Standard Edition, 1995

5. Kinh Thánh, bản của vua James, Cách ngôn 16:11, New American Standard Edition, 1995

6. Mathematics and Measurement, tác giả O.A.W Dilke, 1987

7. The Travels Of Marco Polo, phiên bản tiếng Anh, tác giả Marco Polo (khoảng năm 1300 sau Công nguyên), William Marsden chuyển ngữ, 1818

8. Three Centuries of Harvard, tác giả Samuel Eliot Morison, 1936